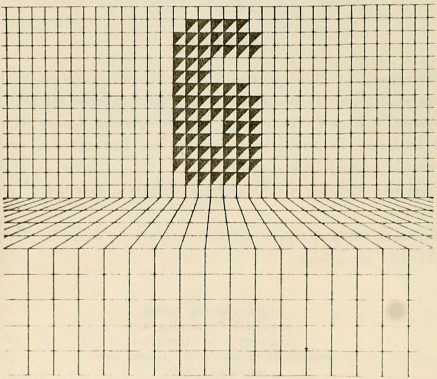
SEXTA
JORNADA DE
MATEMATICA
OCTUBRE 24 - 25 - 26 / 1990
TEMUCO



# ASPECTOS SOBRE LA TEORIA ELEMENTAL DE NUMEROS

## (CURSO B1)

ENZO GENTILE

TEORIA ELEMENTAL DE NUMEROS

ASPECTOS GENERALES DE LA DIVISIBILIDAD

1. PRELIMINARES.

En el estudio de la Aritmética elemental, podemos observar que la noción de divisibilidad en el anillo de los enteros $\mathbb{Z}$ tiene un rol protagónico en el desarrollo de la Teoría de Números. Una de las ideas más fecundas en la historia del desarrollo de la Aritmética ha sido extender la divisibilidad a dominios numéricos, o sea a ampliaciones de $\mathbb{Z}$. Se justifica antonces encarar la divisibilidad en un contexto general. En este Capítulo haremos precisamente un tratamiento general. Luego de consideraciones básicas haremos divisibilidad en el anillo de enteros de Gauss donde la teoría es tan satisfactoria como en $\mathbb{Z}$. En cambio en el anillo numérico $\mathbb{Z}[\sqrt{-5}]$, nos encontramos con un obstáculo: falla la factorización única en producto de elementos irreductibles. ¿Por qué falla? La respuesta la dió Kummer a mediados del siglo pasado: "faltan factores" ... Su remedio fué precisamente definir factores ideales para recomponer la factorización única. Dedekind dió el toque final: los factores ideales son los ideales. Hay que hacer entonces divisibilidad de ideales, que afortunadamente extiende la divisibilidad a nivel de elementos. Esto es, reconquistar el paraíso perdido!!...

Todas las nociones básicas de divisibilidad son válidas en el contexto general de un dominio de integridad. Si con $A$ denotamos un dominio de integridad (o sea: $A$ es un anillo conmutativo, con elemento neutro $1 \neq 0$ y posee

la ley cancelativa: $a \cdot c = a \cdot b$ en $A$, $a \neq 0 \Rightarrow c = b$) dados $a$ y $b$ en $A$, $a \neq 0$ decimos que "a divide a b" si existe $c$ en $A$ tal que $b = a \cdot c$. Escribimos $a|b$. En caso que $a$ no divida a $b$ escribimos $a \not| b$. Si $a$ divide a $b$ decimos que: $a$ es un factor de $b$ ó que $b$ es un múltiplo de $a$ ó que $a$ es un divisor de $b$, etc. Es claro que, como en $\mathbb{Z}$ (el anillo de los enteros racionales) son válidas las propiedades:

i. $a \neq 0$, $a|a$

ii. $a \neq 0$, $b \neq 0$, $a|b$ y $b|c \Rightarrow a|c$.

Adoptaremos, por razones de simplicidad, el criterio que, cuando escribimos $a|b$ se sobreentiende que $a \neq 0$.

Para desarrollar la teoría de divisibilidad en $A$ necesitamos definir los siguientes conceptos primarios.

1.1. $u \in A$ se denomina unidad si es inversible en $A$, es decir, existe $u' \in A$ tal que $u \cdot u' = 1$. Por ejemplo 1 es unidad. La totalidad de unidades de $A$ la denotamos con $U(A)$ o simplemente $U$.

1.2. $a \in A$, $a \neq 0$, $a \notin U$ se dice irreductible en $A$ si $a = b \cdot c$ en $A \Rightarrow b \in U$ ó $b = u \cdot a$ con $u \in U$.

1.3. $a \in A$, $a \neq 0$, $a \notin U$ se dice primo en $A$ si $a|b \cdot c \Rightarrow a|b$ ó $a|c$.

1.4. $a$ y $b$ en $A$ se dicen asociados si existe $u \in U$ tal que $a = u \cdot b$. Escribimos $a \sim b$.

Es claro que un elemento es irreductible si sus divisores son unidades o asociados.

1.5. Ejercicios:

1. Probar que la totalidad $U(A)$ de unidades de $A$ es un grupo, el grupo de unidades de $A$. Problema: determinar la estructura del grupo de unidades de los anillos $A = \mathbb{Z}_n$ de restos módulo $n$.

2. Probar que $a,b$ son asociados sí y sólo si $a|b$ y $b|a$.

3. Probar que, en general, todo elemento primo es irreductible.

4. Probar que en el anillo $\mathbb{Z}$, todo elemento irreductible es primo.

1.6. DEFINICION. Un dominio de integridad $A$ se dice de factorización única (DFU) si para todo elemento $a \in A$ tal que: $a \notin U(A)$, $a \neq 0$ existen elementos irreductibles $q_1, \ldots, q_r$ tales que $a = \prod_1^r q_i$. Además si $p_1, \ldots, p_s$ son elementos irreductibles de $A$ tales que $a = \prod_1^s p_j$ entonces se verifica que $r = s$ y existe una permutación $f$ de $\{1,2, \ldots, r\}$ tal que $q_i$ es asociado de $p_{f(i)}$. Esta última parte se expresa diciendo que la factorización es única.

Dejamos a cargo del lector demostrar:

i. Si $A$ es un DFU entonces todo elemento irreductible es primo. Por lo tanto ambos conceptos coinciden.

ii. Un dominio $A$ es DFU sí y sólo si todo elemento $\neq 0$ y que no es unidad es producto de elementos primos.

1.7. Ejemplos:

1. Dominios de factorización única.

i) $\mathbb{Z}$, el anillo de enteros racionales.

ii) $K[X]$, el anillo de polinomios en $X$ con coeficientes en un cuerpo $K$.

iii) $\mathbb{Z}[X]$, el anillo de polinomios en $X$ con coeficientes enteros

iv) Si $A$ es un DFU entonces $A[X]$ es un DFU.

v) $\mathbb{Z}[i] = \{a + b \cdot i \mid a,b \in \mathbb{Z}, i^2 = 1\}$ = anillo de enteros de Gauss es un DFU como se demostrará más adelante.

vi) Sea $p$ primo racional positivo y sea $A \subset \mathbb{Q}$ la totalidad de números racionales que admiten una representación del tipo

$$\frac{m}{n}, \quad (m,n) = 1, \quad p \nmid n.$$

Es fácil ver que $A$ es un subanillo de $Q$. Las unidades de este anillo la constituyen la totalidad de fracciones irreductibles $\frac{m}{n}$ con $(m,p) = 1$, o sea con numerador y denominador no divisible por $p$. Entonces si $\frac{m}{n}$ es unidad en $A$, $\frac{n}{m} \in A$. Todo elemento de $A$ se expresa unívocamente en la forma

$$p^a \cdot \frac{m}{n} \quad \text{con} \quad a \in \mathbb{Z}, \quad a \geq 0, \quad (m,n) = 1 \quad \text{y} \quad p \nmid m \cdot n .$$

(Esta afirmación es consecuencia de ser $\mathbb{Z}$ un DFU, ¿No?)

El número $p$ es primo en $A$ y es, salvo asociados, el único primo de este anillo. Este ejemplo se generaliza inmediatamente permitiendo que en lugar de $p$ se admita una familia finita o infinita de primos. O sea, si $P$ es una familia no vacía de primos, se define $A$ por la totalidad de racionales que admiten una representación irreductible $\frac{m}{n}$ con $n$ no divisible por ningún primo de la familia $P$.

2. Dominios sin factorización única.

i) Sea $A = \mathbb{Z}[\sqrt{-5}]$, el (sub)anillo de números complejos de la forma $a + b\cdot\sqrt{-5}$ con $a$ y $b$ enteros y $\sqrt{-5}$ denotando un número complejo fijo cuyo cuadrado es -5.

En este anillo todo elemento $\neq 0$ y que no es unidad es producto de elementos irreductibles, pero no en forma unívoca. Sin justificación un tal ejemplo es

$$9 = 3\cdot 3 = (2 + \sqrt{-5})\cdot(2 - \sqrt{-5}) .$$

Los elementos $3$, $2 + \sqrt{-5}$ y $2 - \sqrt{-5}$ son irreductibles pero no son primos. Es fácil ver que 3 no divide ni a $2 + \sqrt{-5}$ ni a $2 - \sqrt{-5}$ aunque divide al producto.

ii) Sea $A = \mathbb{Z}[\sqrt{-3}] = \{a + b\cdot\sqrt{-3} \mid a \text{ y } b \text{ enteros}\}$. Se puede verificar sin dificultad que este anillo no es un DFU. Por ejemplo el elemento 3 es irreductible pero no primo.

iii) Sea $A \subset \mathbb{Q}[X]$ el subanillo formado por todos los polinomios que carecen de término en $X$. O sea $A$ consiste de todos los polinomios de la forma

$$a_0 + a_2X^2 + \ldots + a_nX^n$$

En este anillo los elementos $X^2$ y $X^3$ son irreductibles (pues falta el factor $X$). Además no son asociados dado que las unidades de $A$ son los polinomios constantes no nulos. Por lo tanto

$$X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$$

son dos factorizaciones esencialmente distintas del polinomio $X^6$. Por lo tanto $A$ no es DFU.

iv) El ejemplo de Hilbert.

Este ejemplo sirve para iluminar el fenómeno de la falta de factorización única. Se trata de considerar un conjunto dotado de un producto por el cual todo elemento del mismo es irreductible o producto de irreductible, pero no en forma única. Sea $A$ el conjunto de todos los enteros positivos congruentes a 1 módulo 4:

$$A = 1,5,9,13,17,21,25,29,33,37,41,45,49, \ldots$$

Consideremos en $A$ el producto de enteros. Es claro que $A$ es cerrado respecto de este producto. Se tienen algunas factorizaciones: $25 = 5 \cdot 5$, $45 = 5 \cdot 9$, ... Los números $5,9,13,17,21,29, \ldots$ son irreductibles. Por ejemplo 9 es irreductible "pues nos falta 3".

Si tomamos dos números primos de la forma $4m + 3$ vemos fácilmente que su producto está en $A$. Por ejemplo $3 \cdot 7 = 21 \in A$. por lo tanto

$$441 = 21 \cdot 21 = 3^2 \cdot 7^2 = 9 \cdot 49 .$$

Los números 9, 21, 49 son irreductibles en $A$, por lo tanto la factorización única deja de valer.

Si pensamos en los primos de la forma $4m + 3$ como factores ideales para $A$, entonces la factorización única podría recomponerse, pero claro no a nivel de elementos de $A$.

1.8. Propiedad Fundamental.

Sea $A$ un dominio de factorización única. Como en $\mathbb{Z}$ es posible definir máximo común divisor de dos (o más elementos) de $A$. Dados $a,b \neq 0$, un elemento $d \in A$ se denomina máximo común divisor de $a$ y $b$ si verifica las condiciones:

i) $d|a$ y $d|b$

ii) Si $c|a$ y $c|b$ entonces $c|d$.

Es claro que si $d$ es máximo común divisor de $a$ y $b$ también lo es $u \cdot d$ con $u$ unidad en $A$. También se verifica que dos máximo común divisores de $a$ y $b$ son asociados. Por lo tanto el máximo común divisor, si existe, está univocamente determinado, salvo unidades. Siendo $A$ un DFU, se puede demostrar imitando la demostración hecha en $\mathbb{Z}$, que existe el máximo común divisor de $a$ y $b$. Lo denotamos por abuso de notación con $(a,b)$ pero deberá quedar claro que $(a,b)$ está determinado salvo asociados. Si $a = b = 0$ definimos $(a,b) = 0$. Si el único divisor común a $a$ y $b$ es una unidad decimos que $a$ y $b$ son coprimos y escribimos $(a,b) = 1$.

La propiedad fundamental que interesa en problemas de divisibilidad y que es válida en todo DFU es la siguiente: Sean $a,b,c$ en $A$, $n \in N$. Entonces

$$(a,b) = 1 \ , \ a \cdot b = c^n \Rightarrow \exists \ c_1, c_2 \in A \ , \quad u_1, u_2 \in U(A)$$

tales que $a = u_1 \cdot c_1^n$, $b = u_2 \cdot c_2^n$.

La demostración es una consecuencia trivial de la factorización única en producto de primos.

1.9. La ecuación Pitagórica $x^2 + y^2 = z^2$ .

A manera de aplicación trabajando en $A = \mathbb{Z}$ resolvamos un problema diofántino clásico. A saber, determinaremos todas las soluciones enteras de la ecuación pitagórica $x^2 + y^2 = z^2$ . Es suficiente limitarse a determinar las soluciones primitivas, es decir, tales que $x,y,z$ son positivos y coprimos. Sea entonces $x,y,z$ una solución primitiva a nuestra ecuación. Una primera observación dice que $x$ e $y$ no pueden ser ambos números impares. Basta analizar restos módulo 4 y los detalles quedan como ejercicio. Supongamos entonces que $x$ es par y por lo tanto $y$ es impar. Obviamente $z$ es impar. Se sigue de la ecuación que

$$x^2 = z^2 - y^2 = (z - y)(z + y)$$

y también según lo que acabamos de decir

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z - y}{2}\right).\left(\frac{z + y}{2}\right) \quad \text{en } \mathbb{Z} .$$

Es fácil ver que

$$\frac{z - y}{2} \qquad y \qquad \frac{z + y}{2}$$

son coprimos. (En efecto, si $p$ divide a ambos números divide a la suma, o sea $z$ y a la resta, o sea $y$ , por lo tanto a $x$ , entonces $p = \pm 1$) .

Por la propiedad fundamental de un DFU se sigue que ambos números son, salvo unidades, cuadrados. Pero siendo positivos las unidades deben ser iguales a 1, o sea finalmente

$$\frac{z - y}{2} = a^2 \quad , \qquad \frac{z + y}{2} = b^2 .$$

Por lo tanto

$$\begin{cases} z = b^2 + a^2 \\ y = b^2 - a^2 \\ x = 2ab \end{cases}$$

Siendo $x,y,z$ una solución primitiva, $a$ y $b$ son coprimos y tienen distinta paridad y podemos considerarlos números positivos. Recíproca - mente, dando a $a$ y $b$ valores enteros positivos, coprimos y de dis - tinta paridad obtenemos soluciones primitivas. Esta es pues la solución completa de nuestro problema diofantino.

Esta solución ya aparece en el libro Elementos de Euclides. Veamos una lista de soluciones primitivas de la ecuación $x^2 + y^2 = z^2$ .

| a | b | x | y | z |
|---|---|---|---|---|
| 2 | 1 | 4 | 3 | 5 |
| 3 | 2 | 12 | 5 | 13 |
| 4 | 1 | 8 | 15 | 17 |
| 5 | 2 | 20 | 21 | 29 |
| 5 | 4 | 40 | 9 | 41 |
| 6 | 1 | 12 | 35 | 37 |
| 6 | 5 | 60 | 11 | 65 |
| 7 | 2 | 28 | 45 | 53 |
| 7 | 4 | 56 | 33 | 65 |
| 7 | 6 | 84 | 13 | 85 |

| a | b | x | y | z |
|---|---|---|---|---|
| 8 | 1 | 16 | 63 | 65 |
| 8 | 3 | 48 | 55 | 73 |
| 8 | 5 | 80 | 39 | 89 |
| 9 | 2 | 36 | 77 | 85 |
| 9 | 4 | 72 | 65 | 97 |
| 9 | 8 | 144 | 17 | 130 |
| 10 | 1 | 20 | 99 | 101 |
| 10 | 3 | 60 | 91 | 109 |
| 10 | 7 | 140 | 51 | 149 |
| 10 | 9 | 180 | 19 | 181 |

Utilizando la resolución de la ecuación $X^2 + Y^2 = Z^2$ mostramos que las ecuaciones $X^4 + Y^4 = Z^2$ y $X^4 + Y^4 = Z^4$ , no poseen soluciones enteras positivas. Este ejemplo fue resuelto originalmente por Fermat utilizando su "método del descenso". Notemos que será suficiente probar la irresolubilidad de $X^4 + Y^4 = Z^2$ . Supongamos entonces la existencia de una solución $x,y,z \in \mathbb{N}$ con $z$ mínimo (entre todas las soluciones). El método del descenso consiste en probar que existe <u>otra</u> solución: $x',y',z' \in \mathbb{N}$ con $z' < z$ . Esto es contradictorio y prueba que no exis - ten soluciones. Entonces de $x^4 + y^4 = z^4$ podemos inferir la existencia de $a,b \in \mathbb{N}$ tales que (suponiendo sin pérdida de generalidad que $x$ es par)

$$x^2 = 2ab \quad , \quad (a,b) = 1$$

$y^2 = b^2 - a^2$ , $a$ y $b$ de distinta paridad,

$z^2 = b^2 + a^2$ , supongamos $a$ par.

Entonces $\left(\frac{x}{2}\right)^2 = \frac{a}{2}b$ y como $\left(\frac{a}{2}, b\right) = 1$ existen $r,s \in \mathbb{N}$ tales que $\frac{a}{2} = r^2$ y $b = s^2$. De la ecuación $b^2 = a^2 + y^2$ inferimos la existencia de $i,j \in \mathbb{N}$ tales que

$$a = 2ij$$

$$y = j^2 - i^2 \quad , \quad (i,j) = 1$$

$$b = j^2 + i^2$$

o sea $r^2 = \frac{a}{2} = i \cdot j$. Por lo tanto $i = t^2$ y $j = u^2$, $t,u \in \mathbb{N}$, finalmente $s^2 = b = j^2 + i^2 = t^4 + u^4$ con lo que: $t,u,s$ es otra solución de la ecuación $X^4 + Y^4 = Z^2$.

Pero notemos que: $s \leq s^4 = b^2 < z$! y esto es lo que deseabamos obtener.

Otra consecuencia interesante de la resolución de la ecuación pitagórica $X^2 + Y^2 = Z^2$ es la no existencia de triángulos pitagóricos cuyas áreas sean cuadrados. Es decir no existen triángulos rectángulos de catetos e hipotenusas de longitudes enteras cuyas áreas sean cuadrados. Dicho en otros términos dado un triángulo pitagórico, no existe un cuadrado de lado entero que tenga la misma área.

Sean entonces $a,b,c$ enteros positivos tales que sean coprimos y satisfagan $a^2 = b^2 + c^2$, $bc = 2m^2$, $m \in \mathbb{N}$. Entonces podemos escribir

$$a = x^2 + y^2 \quad , \quad b = 2xy \quad , \quad c = x^2 - y^2 \quad , \quad 0 < y < x \quad , \quad (x,y) = 1 .$$

Se tiene además

$$xy(x^2 - y^2) = m^2$$

y por lo tanto

$$x = X^2 \quad , \quad y = Y^2 \quad , \quad x^2 - y^2 = Z^2 \quad , \quad 0 < Y < X \quad , \quad (X,Y) = 1 .$$

Obtenemos la ecuación

(1) $\quad X^4 - Y^4 = Z^2 .$

y será cuestión de probar la irresolubilidad de esta ecuación en enteros positivos. Supongamos entonces una solución $X,Y,Z$ con $X$ mínimo. Puesto que $X^4 = Y^4 + Z^2$ es claro que $X$ debe ser impar. Podemos escribir:

$$\begin{cases} X^2 = i^2 + j^2 \ , \ Y^2 = i^2 - j^2 \ , \ Z = 2ij \ , \text{ si } Y \text{ es impar} \\ X^2 = i^2 + j^2 \ , \ Y^2 = 2ij \ , \text{ si } Y \text{ es par} \\ \qquad 0 < j < i \ , \ (i,j) = 1 \ . \end{cases}$$

Sea $Y$ impar. Entonces, $X^2Y^2 = i^4 - j^4$ , es una solución de la ecuación (1) con $0 < i < X$ . Una contradicción. Sea $Y$ par. Supongamos SPG que $i$ es par, $j$ impar. Entonces como $Y = 2p$ , se tiene $2p^2 = 2 \cdot \frac{i}{2} j$ y por lo tanto $i = 2r^2$ , $j = s^2$ , $(r,s) = 1$ . O sea $X^2 = 4r^4 + s^4$ , $Y^2 = 4r^2s^2$ o también $Y = 2rs$ . Sean $u,v \in \mathbb{N}$ tales que $X = u^2 + v^2$ , $2r^2 = 2uv$ , $s^2 = u^2 - v^2$ . Entonces $u = t^2$ , $v = h^2$ con lo que $s^2 = t^4 - h^4$ . Pero $t = x^2 < X$ , una contradicción. En conclusión (1) no posee soluciones $X,Y,Z$ en $\mathbb{N}$ .

1.10. Ejemplo. Anillo de polinomios que son DFU.

Probaremos ahora que si $R$ es un dominio de factorización única entonces el anillo de polinomios $R[X]$ con coeficientes en $R$ también es un dominio de factorización única. Para probar este resultado introduciremos la noción de polinomio primitivo.

Supondremos en el resto de esta sección que $R$ es un DFU.

DEFINICION. Un polinomio $f = \sum a_i X^i \in R[X]$ se dice primitivo si el máximo común divisor de $a_1, \ldots, a_n$ es 1.

LEMA. Si $f \in R[X]$ , entonces $f = c \cdot f'$ , con $f' \in R[X]$ primitivo y $c \in R$ , y esta descomposición es única a menos de elementos inversibles. Esto es, si $f = c \cdot f' = c_1 \cdot f_1'$ , con $c, c_1 \in R$ , $f, f_1'$ primitivos, entonces $c \sim c_1$ , $f' \sim f_1'$ .

Demostración: Si $f = \sum_{i=1}^{n} a_i X^i$ y $c = MCD(a_1, \ldots, a_n)$ entonces

$f = c \cdot f'$ , con $f' = \Sigma\, b_i X^i$ , donde $a_i = c \cdot b_i$ . El polinomio $f'$ es primitivo, lo que prueba la existencia de la descomposición. La demostración de la unicidad queda a cargo del lector.

Sea $f = \sum_{i=0}^{n} a_i X^i$ , $g = \sum_{i=0}^{m} b_i X^i$ en $R[X]$ . Entonces $f \cdot g = \sum_{i=0}^{n+m} c_i X^i$ con $c_i = \sum_{j+k=i} a_j b_k$ . Sea $p \in R$ , primo. Supongamos que $p \nmid f$ y $p \nmid g$ . Entonces existen índices $i_0, j_0$ , $0 \leq i_0 \leq n$ , $0 \leq j_0 \leq m$ , mínimos con la propiedad: $p \nmid a_{i_0}$ , $p \nmid b_{j_0}$ . Por lo tanto $p \nmid a_{i_0} b_{j_0}$ . Se sigue entonces que $p \nmid c_{i_0+j_0} = \ldots + a_{i_0} b_{j_0} + \ldots$ Por lo tanto $p \nmid f \cdot g$ y hemos probado:

LEMA. Si $p$ es un primo de $R$ entonces $p$ es un primo de $R[X]$ .

LEMA DE GAUSS. Sean $f, g \in R[X]$ . Entonces el producto $f \cdot g$ es primitivo si y sólo si $f$ y $g$ son primitivos.

Demostración: $\Rightarrow$) Si $f$ no es primitivo y $p$ es un primo de $R$ que divide a los coeficientes de $f$ , entonces $p$ divide a los coeficientes de $f \cdot g$ , luego $f \cdot g$ no es primitivo.

$\Leftarrow$) Supongamos que $f \cdot g$ no es primitivo y sea $p$ un primo de $R$ que divide a $f \cdot g$ . Por Lema sabemos que $p$ es primo en $R[X]$ , luego $p \mid f$ ó $p \mid g$ , de donde $f$ no es primitivo o $g$ no es primitivo.

LEMA. Sea $f$ un polinomio irreductible en $R[X]$ de grado $> 0$ . Entonces $f$ es primitivo e irreductible en $K[X]$ .

Demostración: Sabemos que $f = c \cdot f'$ , con $c \in R$ y $f'$ primitivo. Como $f$ es irreductible entonces $c$ es inversible, luego $f$ es primitivo.

Supongamos ahora que $f = g \cdot h$ , con $g$ y $h \in K[X]$ polinomios de grado $> 0$ , y sean $a_1, a_2 \in R \setminus \{0\}$ tales que $a_1 \cdot h, a_2 \cdot g \in R[X]$ . Entonces $a_1 \cdot a_2 \cdot f = (a_1 h) \cdot (a_2 g) = h_1 g_1$ , con $h_1 g_1 \in R[X]$ . Escribimos $h_1 = b_1 \cdot h'$ , $g_1 = b_2 \cdot g'$ , con $b_1, b_2 \in R$ y $h', g'$ polinomios primitivos. Entonces $a_1 \cdot a_2 \cdot f = b_1 \cdot b_2 \cdot h' \cdot g'$ , donde $f$ y $h' \cdot g'$ son primitivos.

Por lo tanto $f \sim h' \cdot g'$ en $R[X]$, lo que contradice la irreductibilidad de $f$ en $R[X]$. Esto prueba que $f$ es irreductible en $K[X]$.

LEMA. Todo polinomio irreductible $f \in R[X]$ es primo.

Demostración: Sea $f \in R[X]$ un polinomio irreductible.

Si $f$ es de grado cero, entonces $f \in R$ es un elemento irreductible de $R$, por ser irreductible en $R[X]$. Como $R$ es un DFU entonces $f$ es primo en $R$, y hemos probado entonces que $f$ es primo en $R[X]$.

Sea $f$ de grado positivo y sean $g,h \in R[X]$ tales que $f \mid g\,h$. Puesto que $f$ es irreductible en $K[X]$ se tiene que $f \mid g$ ó $f \mid h$ en $K[X]$. Supongamos $f \mid g$, o sea $g = f \cdot t$ en $K[X]$.

Sean $a,a' \in R \setminus \{0\}$ tales que $at \in R[X]$ y $at = a't'$ con $t' \in R[X]$, $t'$ primitivo. Se tiene

$$ag = a'(f \cdot t')$$

con $f \cdot t'$ primitivo. Escribiendo $g = a''g'$, $a'' \in R$ y $g'$ primitivo se sigue que $aa'' \sim a'$, por lo tanto $f \mid g'$ y también $f \mid g$ como queríamos probar.

Podemos ahora probar el resultado buscado.

1.20. PROPOSICION. Si $R$ es un DFU entonces $R[X]$ es un DFU.

Demostración: Sea $f \in R[X]$. Entonces $f = c \cdot f'$, con $c \in R$ y $f'$ primitivo. $c$ se escribe como producto de elementos primos de $R$, y éstos son primos en $R[X]$. Por otro lado, si $f'$ no es irreductible entonces se puede escribir $f' = f_1 \cdot f_2$, con $f_i$ de grado menor que el grado de $f'$, $i = 1,2$. Por el Lema de Gauss sabemos que $f_1$ y $f_2$ son primitivos. Se prueba entonces por inducción que todo polinomio $f \in R[X]$ es producto de polinomios irreductibles. Por el Lema anterior sabemos además que todo irreductible es primo, de donde $R$ es un DFU.

COROLARIO. Si $K$ es un cuerpo entonces el anillo de polinomios $K[X_1, \ldots, X_n]$ en las indeterminadas $X_1, \ldots, X_n$, es un DFU.

Demostración: $K[X_1]$ es un DFU. Además $K[X_1, \ldots, X_n] = K[X_1, \ldots, X_{n-1}][X_n]$ si $n > 1$.

1.11. Ejemplo. Anillos numéricos.

Una familia importante de dominios de integridad y a la vez de relevancia histórica la constituyen los anillos de enteros algebraicos. Será necesario dar algunas definiciones.

Un número complejo $a$ se dice algebraico (sobre $Q$!) si existe un polinomio no nulo $f(X) \in Q[X]$ (coeficientes racionales) tal que $f(a) = 0$. Por ejemplo todo $r \in Q$ es algebraico: satisface la ecuación racional $X - r = 0$. El número irracional $\sqrt{2}$ es algebraico: satisface la ecuación $X^2 - 2 = 0$.

En cambio los números reales $e$, $\pi$, $2^{\sqrt{2}}$ no son algebraicos. Los números complejos que no son algebraicos se denominan trascendentes. Sea $K$ un cuerpo contenido en $C$, o mejor dicho un subcuerpo de $C$. Es claro que $K$ contiene al cuerpo racional. Se dice entonces que $K$ es una extensión de $Q$. Se dice que $K$ es una extensión algebraica de $Q$ si todo elemento de $K$ es algebraico (sobre $Q$). Puesto que $K$ es un espacio vectorial sobre $Q$, se denomina grado de $K$ a la dimensión de $K$ como espacio vectorial sobre $Q$. Si esa dimensión es finita se dice que $K$ es una extensión finita o de grado finito. El siguiente procedimiento da las extensiones finitas de $Q$. Sea $f(X)$ un polinomio en $Q[X]$, irreductible de grado $r$. Sea $\alpha$ una raíz compleja de $f(X)$. Entonces la totalidad de números complejos de la forma

$$a_0 + a_1\alpha + \ldots + a_{r-1}\alpha^{r-1} \qquad \text{con } a_i \text{ en } Q,$$

es un cuerpo, que denotamos con $Q(\alpha)$, de grado $r$ sobre $Q$.

Otro concepto importante es el de entero algebraico. Un número complejo $a$ se dice entero algebraico, si existe un polinomio $f(X) \in \mathbb{Z}[X]$, de grado positivo, con coeficientes enteros y MONICO tal que $f(a) = 0$. Los enteros algebraicos son números algebraicos pero no necesariamente

a la inversa.

Dada una extensión algebraica $K$ de $Q$, la totalidad de elementos de $K$ que son enteros algebraicos constituyen un ANILLO (no un cuerpo) $S$ que se denomina el anillo de enteros (algebraicos) de $K$. La filosofía de la Teoría Algebraica de Números es que $K$ y $S$ juegan el papel de $Q$ y $Z$, respectivamente. Conforman el diagrama


$K$ generaliza $Q$ y $S$ generaliza $Z$. Se trata entonces de hacer divisibilidad en $S$ y que la aritmética de $S$ ayude a entender y a desarrollar la aritmética racional (en $Z$). Por ejemplo, la famosa conjetura de Fermat (si $n > 2$ no existen enteros positivos $x,y,z$ tales que $x^n + y^n = z^n$) ha sido estudiada trabajando no en $\mathbb{Z}$ sino en el cuerpo ciclotómico $Q(\xi)$, con $\xi$ una raíz n-sigma primitiva de la unidad. Los enteros algebraicos de este anillo son la totalidad de expresiones polinomiales en $\xi$ con coeficientes enteros.

Mencionemos explícitamente una familia importante de ejemplos, a saber las extensiones cuadráticas. Son las asociadas a los polinomios $X^2 - d$, con $d$ entero libre de cuadrados. Se tiene

$$Q(\sqrt{d}) = \{r + s\sqrt{d} | r,\ s \in Q\}.$$

Sea $d \in \mathbb{Z}$, $d \neq 0$ no divisible por ningún cuadrado $> 1$. Por ejemplo $-6, -5, -3, -2, -1, 2, 3, 5, 6, \ldots$ Sea $Q(\sqrt{d}) := \{a + b\sqrt{d} | a,b \in Q\}$. $Q(\sqrt{d})$ es un cuerpo, el cuerpo cuadrático de la ecuación $X^2 - d = 0$.

El anillo de enteros de $Q(\sqrt{d})$ es

$$\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a,b \in \mathbb{Z}\} \quad \text{si } d \equiv 2 \text{ ó } 3 \pmod 4$$

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] := \{a + b\frac{1+\sqrt{d}}{2} \mid a,b \in \mathbb{Z}\} \quad \text{si } d \equiv 1 \pmod 4$$

Probemos esta afirmación. Para ello observemos que todo elemento $r + s\sqrt{d} \in Q(\sqrt{d})$ es raíz del polinomio

$$(1) \quad (X - (r + s\sqrt{d}))\cdot(X - (r - s\sqrt{d})) = X^2 - 2rX + r^2 - ds^2 \in Q[X] .$$

Si $r + s\sqrt{d} \notin Q$, entonces el polinomio (1) es irreductible. Por lo tanto $r + s\sqrt{d}$ es entero sí y sólo si:

$$(2) \quad 2r \in \mathbb{Z} \quad \text{y} \quad r^2 - ds^2 \in \mathbb{Z}.$$

De estas dos proposiciones deduciremos la afirmación.

De (2) se sigue que

$$r = \frac{a}{2} \quad \text{con } a \in \mathbb{Z} \quad \text{y} \quad (2r)^2 - d(2s)^2 \in 4\mathbb{Z}.$$

Por lo tanto $d(2s)^2 \in \mathbb{Z}$. Puesto que $d$ es libre de cuadrados se sigue de la factorización única en $\mathbb{Z}$ que $2s \in \mathbb{Z}$, o sea $s = \frac{b}{2}$. Por lo tanto resulta

$$(3) \quad a^2 \equiv db^2 \pmod 4 .$$

Razonemos ahora con restos módulo 4 usando la siguiente información

$$\begin{array}{l} x : 0\ 1\ 2\ 3 \\ x^2 : 0\ 1\ 0\ 1 \end{array} \pmod 4 .$$

Sea $d \equiv 1 \pmod 4$. Se sigue de (3) y de la tabla de restos mod 4 que

$$a \equiv b \pmod 2$$

es decir, $a$ y $b$ tienen la misma paridad. Esto prueba que en este caso los enteros de $Q(\sqrt{d})$ son de la forma

$$\frac{a + b\sqrt{d}}{2} = \frac{(a - b)}{2} + \frac{1 + \sqrt{d}}{2}(a + b)$$

es decir, combinación lineal entera de 1 y $\frac{1 + \sqrt{d}}{2}$ .

Sea $d \equiv 2,3 \pmod 4$ . Entonces (3) se verifica sí y sólo si $a \equiv b \equiv 0 \pmod 2$ es decir a y b son enteros pares. En estos dos casos los enteros algebraicos de $Q(\sqrt{d})$ son de la forma

$$x + y\sqrt{d} \quad , \qquad x \text{ e } y \text{ en } \mathbb{Z} .$$

La afirmación queda completamente demostrada.

1.12. Una aplicación.

Fijemos las ideas de analizar problemas diofantinos en un ámbito más grande que el ordinario de $\mathbb{Z}$ , estudiando las soluciones enteras de la ecuación $x^2 - 3y^2 = 1$ . Geométricamente se trata de hallar todos los puntos (x,y) de $R^2$ de coordenadas enteras pertenecientes a la hipérbola $x^2 - 3y^2 = 1$ . Aritméticamente se trata de hallar todas las bases y de numeración tales que el número 301 (escrito en base y) sea un cuadrado.

En lugar de resolver el problema en $\mathbb{Z}$ lo resolveremos trabajando en $A = \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \,/\, a,b \in \mathbb{Z}\}$ que es el anillo de enteros del cuerpo cuadrático $Q(\sqrt{3})$ . Se tiene. $1 = x^2 - 3y^2 = (x - \sqrt{3}\cdot y)$ . $(x + \sqrt{3}\cdot y)$ y el problema se transforma ahora en la determinación de los elementos $z \in A = \mathbb{Z}[\sqrt{3}]$ que son unidades (o sea $z\cdot z' = 1$ , para algún $z'$ en A) . Por ejemplo uno observa que el elemento $2 + \sqrt{3}$ es unidad: $(2 + \sqrt{3})\cdot(2 - \sqrt{3}) = 1 = 2^2 - 3\cdot 1^2$ . Luego (2,1) es una solución a nuestro problema.

Pero si $u \in A$ es unidad también lo son todas las potencias $u^i$ , i natural y aún más $\pm u^i$ , i entero, de manera que el problema tiene infinitas soluciones. Por ejemplo

$$(2 + \sqrt{3})^2 = 7 + 4\sqrt{3} \quad \text{dá la solución } x = 7 , \; y = 4$$

$(2 + \sqrt{3})^3 = 26 + 15\sqrt{3}$ dá la solución $x = 26$ , $y = 15$ .

La teoría de unidades en cuerpos numéricos nos dice que (todas) las unidades de $\mathbb{Z}[\sqrt{3}]$ son precisamente de la forma $\pm(2 + \sqrt{3})^i$ , $i$ entero, de manera que el problema queda completamente resuelto. Como lección de este ejemplo podemos derivar la importancia de conocer el grupo $U(A)$ de unidades de un dominio, por ejemplo, de números algebraicos.

1.13. Digresión general.

Digamos que la llamada Teoría Algebraica de Números tiene por objeto estudiar la divisibilidad en dominios numéricos tales como el anillo de enteros algebraicos de una extensión algebraica finita de $\mathbb{Q}$ . Le interesa saber por ejemplo si tal dominio es un DFU y en el caso de no serlo se pregunta en cuánto se aleja de un DFU. El llamado número de clases mide esta divergencia. Los cuerpos con números de clases igual a 1 son los DFU. Un problema concreto que ya aparece en Disquisitiones Arithmeticae, obra cumbre de C.F. Gauss conjetura que para cuerpos cuadráticos $\mathbb{Q}(\sqrt{d})$ con $d < 0$ , los únicos cuyos anillos de enteros algebraicos, que son DFU ocurren para $d = 3,-2,-1,-7,-11,-19,-43,-67,-163$ y para ningún otro $d < -163$ . En 1922 se demostró que había a lo sumo 10 cuerpos cuadráticos imaginarios (o sea $d < 0$) de factorización única. En 1966-67 Baker y Stark probaron que no existía un décimo cuerpo imaginario con factorización única, concluyendo la solución de esta conjetura de Gauss.

2. ANILLO DE ENTEROS DE GAUSS.

2.1. DEFINICION. $A = \mathbb{Z}[i] := \{a + b\cdot i \mid a,b \in \mathbb{Z}\}$ = anillo de enteros de Gauss. Es fácil ver que $A$ es un dominio de integridad. Es nuestro interés hacer divisibilidad en $A$ a la manera de $\mathbb{Z}$ . Para evitar confusiones, a los elementos de $\mathbb{Z}$ los calificaremos de racionales, tales como enteros racionales, primos racionales. En cambio hablaremos de primos de Gauss

refiriendonos a los elementos de $\mathbb{Z}[i]$ que son primos.

2.2. DEFINICION. Sea $Q(i)$ := la totalidad de números complejos de la forma $a + b \cdot i$ con $a,b \in Q$ .

2.3. Ejercicio. Probar que $Q(i)$ es un cuerpo (o sea, todo elemento no nulo es inversible en $Q(i)$). Probar que $Q(i)$ es cuerpo de cuociente de $\mathbb{Z}[i]$ (es decir, todo elemento $z \in Q(i)$ se escribe como cuociente de enteros de Gauss).

Una función de juega un papel fundamental en el estudio de este tipo de anillos es la norma.

2.4. DEFINICION. La función $N : Q(i) \to Q$ definida por $N(z) = a^2 + b^2$ , si $z = a + b \cdot i$ , se denomina Norma de la extensión $Q(i)$ o simplemente norma.

2.5. DEFINICION. Si $z = a + b \cdot i \in Q(i)$ denotamos con $\bar{z}$ el número complejo $a - b \cdot i$ y lo llamamos el conjugado de $z$ .

2.6. PROPOSICION. Sean $z, z_1, z_2$ en $Q(i)$ .

i) $N(z) = z \cdot \bar{z} = N(\bar{z})$ .

ii) $N(z) = 0$ sí y sólo si $z = 0$

iii) $z \neq 0 \Rightarrow N(z) > 0$

iv) $z \in \mathbb{Z}[i] \Rightarrow N(z) \in \mathbb{Z}$

v) $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$

vi) Sean $z_1 \cdot z_2$ en $\mathbb{Z}[i]$ . Entonces $z_1 \mid z_2$ en $\mathbb{Z}[i]$ implica $N(z_1) \mid N(z_2)$ en $\mathbb{Z}$ .

Demostración: Queda como ejercicio.

2.7. PROPOSICION. $U(\mathbb{Z}[i]) = \{1,-1,i,-i\}$ .

Demostración: En efecto, $z = z_1 \cdot z_2 \Rightarrow N(z) = N(z_1) \cdot N(z_2)$ . Por lo tanto $z_1 \cdot z_2 = 1$ sí y sólo si $N(z_1) \cdot N(z_2) = N(1) = 1$ . O sea, equivale a re-

solver la ecuación $(a^2 + b^2)\cdot(c^2 + d^2) = 1$ , es decir $a^2 + b^2 = 1$ y $c^2 + d^2 = 1$ . Es claro que las únicas soluciones enteras son $a = +1,-1$ y $b = 0$ ó $a = 0$ y $b = +1,-1$ .

En definitiva las unidades de $\mathbb{Z}[i]$ son $1,-1,i,-i$ .

2.8. Ejemplo. $2 = 2 + 0\,i$ no es irreductible en $\mathbb{Z}[i]$ . En efecto, $2 = (1 + i)\cdot(1 - i)$ y claramente $1 + i$ no es ni asociado a 2 ni unidad de $\mathbb{Z}[i]$ .

2.9. Ejemplos. $5 = 5 + 0\cdot i$ no es irreductible en $\mathbb{Z}[i]$ . En efecto, $5 = 2^2 + 1 = (2 + i)\cdot(2 - i)$ .

2.10. Ejemplo. $3 = 3 + 0\cdot i$ es primo en $\mathbb{Z}[i]$ . En efecto, sea $z_1\cdot z_2 = 3\cdot z_3$ en $\mathbb{Z}[i]$ . Tomando norma $(a^2 + b^2)\cdot(c^2 + d^2) = 3m$ con $m$ en $\mathbb{Z}$ ($z_1 = a + b\cdot i$ , $z_2 = c + d\cdot i$) . Siendo 3 primo en $\mathbb{Z}$ divide a uno de los factores, digamos, a $a^2 + b^2$ . Pero, es una propiedad bien conocida de 3 que divide a $a$ y divide a $b$ por lo tanto $3|z_1$ , como queríamos probar. El lector puede intuir un problema natural que sale a luz: ¿Qué primos racionales (o sea en $\mathbb{Z}$) son primos de Gauss? Nuestro próximo paso será probar la existencia de un algoritmo de división en $\mathbb{Z}[i]$ .

2.11. Ejercicios:

i) Probar que todo elemento $z = r + s\cdot i \in Q(i)$ satisface la ecuación $X^2 - 2rX + (r^2 + s^2) = 0$ . (Ecuación característica de $z$)

ii) Probar que $\mathbb{Z}[i]$ es el anillo de enteros algebraicos de $Q(i)$

iii) ¿Contradice la igualdad $2 = (1 + i)\cdot(1 - i) = i\cdot(1 + i)^2$ la factorización única en $\mathbb{Z}[i]$ ?

3. ALGORITMO DE DIVISION EN $\mathbb{Z}[i]$ . TEOREMA FUNDAMENTAL.

En general dado un dominio de integridad $A$ se llama algoritmo de división en $A$ a toda aplicación $t : A - \{0\} \to \mathbb{Z}$ con las propiedades siguientes:

1. $a|b \Rightarrow t(a) \leq t(b)$

ii. Dados a y b , $b \neq 0$ existen q,r en A tales que $a = b \cdot q + r$ con $r = 0$ ó $0 \leq t(r) < t(b)$ .

(Nota: no suponemos ni afirmamos unicidad de q y r como en el algoritmo de división en $\mathbb{Z}$!!) . En general no es cierto que todo dominio de integridad admita algún algoritmo de división. Ya daremos ejemplos.

En el caso de $\mathbb{Z}[i]$ , la norma permite definir un algoritmo de división. Veamos a tal fin el siguiente Lema clave:

3.1. LEMA DE APROXIMACION. Sea $z \in Q(i)$ . Existe $g \in \mathbb{Z}[i]$ tal que $N(z - g) < 1$ .

Demostración: Sea $z = r + z \cdot i$ , $r,s \in Q$ y sea $g = a + b \cdot i$ . Entonces (*) $N(z - g) < 1$ sí y sólo si $(r - a)^2 + (s - b)^2 < 1$ . Sea $a \in \mathbb{Z}$ con $|a - r| \leq \frac{1}{2}$ y análogamente sea $b \in \mathbb{Z}$ tal que $|b - s| \leq \frac{1}{2}$ . Es claro que con esa elección se satisface la equivalencia (*) y el Lema queda probado. Interesa notar que la elección de a y b no es única como se puede apreciar en el gráfico. Notar que $\sqrt{N(z - g)}$ es la distancia euclídea de z a g .

A : 4 elecciones

B : 3 elecciones

C : 2 elecciones

3.2. TEOREMA. La aplicación norma $N : \mathbb{Z}[i] \to \mathbb{Z}$ define sobre $\mathbb{Z}[i]$ un algoritmo de división. O sea $\mathbb{Z}[i]$ es DE (Dominio Euclidiano)

Demostración: Dados $s,t \in \mathbb{Z}[i]$ , $t \neq 0$ , vamos a probar la existencia de q,r en $\mathbb{Z}[i]$ , tales que $s = t \cdot q + r$ con $N(r) < N(t)$ . Para ello aplicamos el Lema de Aproximación a $u = \frac{s}{t}$ y de allí se sigue inmediatamente.

Nota: Las mismas consideraciones permiten probar que $\mathbb{Z}[\sqrt{d}]$ es un dominio euclídeo si $d = -2,2,3$ y $\mathbb{Z}\left[\frac{1 + \sqrt{-3}}{2}\right]$ .

3.3. Ejemplos.

i) Sean $z_1 = 112 + i$ , $z_2 = -57 + 79i$ .

$$\frac{112 + i}{-57 + 79i} = \frac{-(112 + i)(57 + 79i)}{9420} = -\frac{6305 + 8905i}{9420} =$$

$$= (\text{aprox}) -0.66 - 0.93i$$

Tomamos como entero de Gauss aproximante a $-1 - i$ . Se tiene

$$112 + i = (-57 + 79i)\cdot(-1 - i) + (-24 + 23i) ,$$

$$N(-24 + 23i) = 1105 < N(-57 + 79i) = 9490 .$$

ii) Sean $z_1 = -57 + 79i$ , $z_2 = -24 + 23i$

$$\frac{-57 + 79i}{-24 + 23i} = \frac{-(-57 + 79i)(24 + 23i)}{1105} = \frac{3185 - 587i}{1105} =$$

$$= (\text{aprox}) 2.88 - 0.53i$$

Tomamos como entero de Gauss aproximante a $3 - i$ . Se tiene

$$-57 + 79i = (-24 + 23i)\cdot(3 - i) + (-8 - 14i) ,$$

$$N(8 + 14i) = 260 < 1105 = N(-24 + 23i)$$

iii) Sean $z_1 = 24 + 23i$ , $z_2 = 8 + 14i$

$$\frac{-24 + 79i}{8 + 14i} = \frac{(-24 + 23i)(8 - 14i)}{260} = \frac{130 + 520i}{260} = \frac{1}{2} + 2i$$

Tomamos como entero aproximante a $1 + 2i$ . Se tiene

$$-24 + 23i = (8 + 14i)(1 + 2i) + (-4 - 7i) ,$$

$$N(4 + 7i) = 65 < 260 = N(8 + 14i) .$$

Notemos que $4 + 7i \mid 8 + 14i$ .

Estos cálculos los utilizaremos más adelante para calcular el máximo común divisor de $112 + i$ y $-57 + 79i$ .

El algoritmo de división nos servirá para probar un "Teorema Fundamental de la Aritmética" en $\mathbb{Z}[i]$ . O sea,

3.4. Teorema Fundamental de la Aritmética en $\mathbb{Z}[i]$ .

Todo entero de Gauss $g$ que no es ni cero ni unidad es irreductible o puede expresarse como producto de irreductibles $r_i$ , $i = 1, \ldots, n$

$$g = r_1 \cdots r_n .$$

Además, si $g$ admite otra representación

$$g = s_1 \cdots s_m$$

en producto de irreductibles, se verifica que $n = m$ y cada $r_i$ es asociado a un $s_j$ y recíprocamente. O sea, la factorización es esencialmente única.

Demostración: Supongamos el Teorema falso. Existe entonces un elemento $g \in \mathbb{Z}[i]$ , que es distinto de cero, no es unidad, ni es irreductible que no es producto de elementos irreductibles. Entre tales elementos podemos elegir uno $g$ , que posea norma $N(g)$ mínima. Esto es posible pues la norma toma valores no negativos. Podemos escribir entonces $g = g_1 \cdot g_2$ , con factores $g_1$ que no son unidades. Por lo tanto $N(g) = N(g_1) \cdot N(g_2)$ y consecuentemente $1 < N(g_1) < N(g)$ , $1 < N(g_2) < N(g)$ . Pero entonces $g_1$ y $g_2$ son irreductibles o producto de irreductibles y por lo tanto así lo es $g$ , una contradicción. Para probar la unicidad hacemos uso del siguiente Lema.

3.5. LEMA. Sea $q \in \mathbb{Z}[i]$ irreductible y sean $r,s$ enteros de Gauss tales que $q|r \cdot s$ . Entonces $q|r$ ó $q|s$ . O sea todo irreductible es primo.

Demostración: Supongamos elegido un producto $r \cdot s$ en $\mathbb{Z}[i]$ con la propiedad que $q|r \cdot s$ , $q \nmid r$ , $q \nmid s$ , con $N(r)$ mínimo. Existen, según el algoritmo de división, $t,r'$ en $\mathbb{Z}[i]$ tales que $q = r \cdot t + r'$ , con $r' \neq 0$ , pues $q$ es irreductible y $N(r') < N(r)$ . De $q \cdot s = r \cdot s \cdot t + r' \cdot s$ se sigue que $q|r' \cdot s$ . Pero por razones de minimalidad debe verificarse que $q|r'$ , de donde $N(q) \leq N(r') < N(r)$ .

Sea $r = q \cdot t' + r''$ , $r'' \neq 0$ y $N(r'') < N(q)$ . Entonces por un razona-

miento análogo al de más arriba, $q|r''\cdot s$ y por lo tanto $q|r''$ . Se sigue que $N(q) \leq N(r'') < N(q)$ , un absurdo. Provino de suponer $q \not\sim r$ y $q \not\sim s$ . El Lema queda probado.

El Teorema Fundamental de la Aritmética en $\mathbb{Z}[i]$ se sigue inmediatamente de este Lema utilizando el mismo razonamiento en $\mathbb{Z}$ . Dejamos los detalles a cargo del lector.

4. APLICACION. Existencia de máximo común divisor en $\mathbb{Z}[i]$ .

Como en el caso de $\mathbb{Z}$ o de $K[X]$ (K un cuerpo) probamos, vía el algoritmo de división, la existencia de máximo común divisor.

4.1. DEFINICION. Sean $z_1, z_2 \in \mathbb{Z}[i]$ . Se llama máximo común divisor de $z_1$ y $z_2$ a todo $z \in \mathbb{Z}[i]$ con las siguientes propiedades:

i) $z|z_1$ y $z|z_2$

ii) $\forall\, w \in \mathbb{Z}[i]$ , $w|z_1$ y $w|z_2 \Rightarrow w|z$ .

Notemos que si $z$ es máximo común divisor de $z_1$ y $z_2$ entonces: $-z$, $iz$, $-iz$ son también máximo común divisor de $z_1$ y $z_2$ . Escribiremos $mcd(z_1,z_2)$ para denotar algún máximo común divisor de $z_1$ y $z_2$ cuya existencia probamos a continuación.

4.2. TEOREMA. Todo par de enteros de Gauss $z_1, z_2$ , no simultáneamente nulos, posee un máximo común divisor. Si $z = mcd(z_1,z_2)$ existen enteros de Gauss $w_1, w_2$ tales que $z = w_1 z_1 + w_2 z_2$ .

Demostración: Sea $z_2 \neq 0$ . Por el algoritmo de división en $\mathbb{Z}[i]$ resulta:

$$z_1 = z_2 \cdot q_1 + r_0 \quad , \quad N(r_0) < N(z_2)$$

$$r_0 = 0 \text{ ó } z_2 = r_0 \cdot q_2 + r_1 \quad , \quad N(r_1) < N(r_0)$$

$$r_1 = 0 \text{ ó } r_0 = r_1 \cdot q_3 + r_2 \quad , \quad N(r_2) < N(r_1)$$

.....

El proceso es finito dado que los $N(r_i)$ son enteros no negativos y satisfacen

$$N(r_0) > N(r_1) > \dots$$

Por lo tanto termina en algún $r_i \neq 0$ tal que $r_{i+1} = 0$.

Como en el caso de $\mathbb{Z}$:

$$\text{mcd}(z_1,z_2) = \text{mcd}(z_1,r_0)$$

$$\text{mcd}(z_2,r_0) = \text{mcd}(r_0,r_1)$$

.....

por lo tanto si $r_i \neq 0$ y $r_{i+1} = 0$ es $r_i$ un $\text{mcd}(z_1,z_2)$.

Como en el caso de $\mathbb{Z}$ producimos a partir de $r_i$ una combinación lineal de $z_1,z_2$, el teorema queda demostrado.

4.3. Ejemplo: Calculemos $\text{mcd}(112 + i, -57 + 79i)$. Para ello utilizaremos los cálculos hechos al ejemplificar la existencia de algoritmo de división (ver 3.3)

$$112 + i = (-57 + 79i)\cdot(-1 - i) + (-24 + 23i)$$

$$-57 + 79i = (-24 + 23i)\cdot(3 - i) + (-8 + 14i)$$

$$-24 + 23i = (8 + 14i)\cdot(1 + 2i) + (-4 - 7i)$$

$$8 + 14i = (4 + 7i)\cdot 2$$

por lo tanto $4 + 7i$ ($\delta$ $-4 - 7i$ $\delta$ $7 - 4i$ $\delta$ $-7 + 4i$) es máximo común divisor de $112 + i$ y $-57 + 79i$. Se tiene:

$$112 + i = (-7 + 4i)\cdot(-12 - 7i) = (7 - 4i)\cdot(12 + 7i)$$

$$-57 + 79i = (-7 + 4i)\cdot(11 - 5i) = (7 - 4i)\cdot(-11 + 5i)\,.$$

4.4. Ejercicios.

i) Calcular $\text{mcd}(-23 + 2i, 13i)$. (Sol. $3 + 2i$).

ii) Sean $z_1,z_2 \in \mathbb{Z}[i]$ no simultáneamente iguales a cero. Probar que $\text{mcd}(z_1,z_2) = w_1z_1 + w_2z_2$ donde $w_1z_1 + w_2z_2$ es un elemento de

norma positiva mínima entre todos los posibles enteros de Gauss de la forma $r \cdot z_1 + s \cdot z_2$ con $r,s \in \mathbb{Z}[i]$ .

iii) Sean a,b en $\mathbb{Z}$. Probar que $(a,b) = 1$ en $\mathbb{Z}$ si y sólo si $(a,b) = 1$ en $\mathbb{Z}[i]$

5. APLICACION.

La idea de hacer aritmética en $\mathbb{Z}[i]$ es original de Gauss quien la utilizó para el estudio de las llamadas leyes de reciprocidad, cuadrática y bicuadrática. La misma marca un jalón en la historia de la teoría de números al abrir el paso a la gran familia de anillos numéricos. Como hicimos con la ecuación diofantina $X^2 + Y^2 = Z^2$ vamos a resolver ahora otro problema del mismo tipo. A saber hallaremos la totalidad de soluciones enteras de la ecuación $Y^2 + 4 = X^3$ siguiendo las líneas del ejemplo anterior pero ahora haciendo Aritmética en $\mathbb{Z}[i]$ . Para convertir el problema dado en un problema de divisibilidad escribimos, en $\mathbb{Z}[i]$ :

$$(y + 2i) \cdot (y - 2i) = x^3 .$$

Sea p un primo (de Gauss) que divide a $y + 2i$ y a $y - 2i$ . Por lo tanto p divide a $2y$ y a $2i$ . O sea divide a 2. Entonces p es asociado a $1 + i$ . (Recordar que $2 = i\,(1 + i)^2$) .

Supongamos y impar. Entonces $1 + i \mid y + 2i$ , $1 + i \mid 2 = 1 + i \mid y$ . Por lo tanto $y = (1 + i) \cdot t$ en $\mathbb{Z}[i]$ . Tomando norma resulta $y^2 = 2 \cdot N(t)^2$ , en $\mathbb{Z}$. Pero entonces y es par, un absurdo. Concluimos que $(y + 2i)$ y $(y - 2i)$ son coprimos. Por lo tanto, utilizando la propiedad fundamental de un DFU

$$y + 2i = u \cdot (a + b \cdot i)^3 \qquad \text{con } u \text{ , unidad}$$

Ahora dado que todas las unidades en $\mathbb{Z}[i]$ son cubos: $1 = 1^3$ , $1 = (-1)^3$ $i = (-i)^3$ , $-i = i^3$ , podemos absorver u en $(a + b \cdot i)^3$ y suponer sin pérdida de generalidad, que $u = 1$ . Entonces

$$y + 2i = (a + b \cdot i)^3 = a^3 - 3ab^2 + (3a^2b - b^3) \cdot i$$

o sea

$$y = 3a^2b - b^3 = b(3a^2 - b^2)$$

$$2 = a^3 - 3ab^2 = a(a^2 - 3b)$$

La segunda ecuación da por solución $a = 2$, $b = 1$ y por lo tanto $y = 11$. Supongamos ahora que $y$ es par, $y = 2Y$. Notar que $Y$ es impar! Escribiendo $z = 2Z$ resulta la ecuación

$$Y^2 + 1 = 2Z^3 .$$

Por lo tanto, en $\mathbb{Z}[i]$

$$(Y + i)(Y - i) = 2Z^3$$

y también dado que $2 = (1 + i)\cdot(1 - i)$

$$\frac{Y + i}{1 + i}\,\frac{Y - i}{1 - i} = Z^3 .$$

El único divisor primo que podría dividir a ambos factores de la izquierda es $1 + i$. En ese caso $Y + i$ sería divisible por 2, por lo tanto $Y$ sería par, lo cual hemos observado más arriba, no es así.

Concluimos como antes que esos factores son coprimos y por lo tanto

$$\frac{Y + i}{1 + i} = (a + b\cdot i)^3 = a^3 - 3ab^2 + (3a^2b - b^3)i$$

o sea $\quad Y + i = a^3 - 3ab^2 - 3a^2b + b^3 + (a^3 - 3ab^2 + 3a^2b - b^3)i$

Por lo tanto $\quad 1 = a^3 + 3a^2b - 3ab^2b^3 = (a - b)(a^2 + ab + b^2 + 3ab)$

$$= (a - b)(a^2 + 4ab + b^2)$$

Entonces $\quad 1 = a - b$

$$1 = a^2 + 4ab + b^2$$

Se tiene $\quad 1 = (b + 1)^2 + 4b(b + 1)b^2 = 0 = 6b(b + 1)$, $\underline{b = -1}$, $\underline{a = 0}$

Por lo tanto $Y = 1$ y por lo tanto $y = 2$.

En definitiva las soluciones son $\underline{y = 11, z = 5}$ e $\underline{y = 2, z = 2}$.

6. PRIMOS DE GAUSS.

Nos proponemos hallar en esta sección los enteros de Gauss que son primos, es decir, aquellos que hemos llamado primos de Gauss. Notemos primeramente las siguientes propiedades cuya verificación dejamos a cargo del lector.

1. Si $a + b\cdot i$ es primo de Gauss así lo es su conjugado $a - b\cdot i$ .

2. Si $a + b\cdot i \mid a$ , con $a$ entero racional entonces también $a - b\cdot i \mid a$ .

3. $a + b\cdot i$ es asociado a algún entero racional sí y sólo si $a = 0$ ó $b = 0$ .

6.1. PROPOSICION. Si $a + b\cdot i$ posee norma igual a un primo racional entonces es primo de Gauss.

Demostración: Sea $z = a^2 + b^2 = N(a + b\cdot i) = p$ primo racional positivo. Si $z = x\cdot y$ en $\mathbb{Z}[i]$ se tiene tomando norma: $N(z) = N(x)\cdot N(y) = p$ . Esto implica que $N(x) = p$ , $N(y) = 1$ ó $N(x) = p$ y $N(y) = 1$ . Esto prueba bien que $z$ es primo de Gauss.

Se sigue de esta Proposición que los enteros de Gauss $a + b\cdot i$ tales que $a^2 + b^2 = 2$ son primos de Gauss. Estos son exactamente $1 + i$ , $1 - i$ , $-1 + i$ , $-1 - i$ todos asociados entre sí.

Al igual, si $p$ es un primo suma de dos cuadrados: $p = a^2 + b^2$ entonces $a + b\cdot i$ , $-a + b\cdot i$ , $a - b\cdot i$ , $-a - b\cdot i$ son primos de Gauss, todos asociados entre sí.

Veamos qué primos de Gauss verifican la recíproca de la Proposición anterior.

6.2. PROPOSICION. Sea $z = a + b\cdot i$ con $a \neq 0$ y $b \neq 0$ . Entonces $z$ es primo de Gauss sí y sólo si $N(z)$ es primo racional.

Demostración: Sea $z$ primo de Gauss. Si $N(z) = a^2 + b^2 = m\,n$ con $n > 1$ , $m > 1$ , o sea $(a + b\cdot i)\cdot(a - b\cdot i) = m\,n$ , se sigue de ser $\mathbb{Z}[i]$ un dominio de factorización única que $a + b\cdot i$ y (digamos) $m$ deben ser asociados. Esto es un absurdo pues implica $a = 0$ ó $b = 0$ . La recíproca se sigue de 6.1.

Hemos pues caracterizado los primos de Gauss de la forma $a + b\cdot i$ con $a \neq 0$ y $b \neq 0$. Se trata entonces de caracterizar los primos racionales que son primos de Gauss.

6.3. PROPOSICION. Sea $p \in \mathbb{N}$ un primo racional. Entonces $p$ es primo de Gauss sí y sólo si $p$ no es suma de dos cuadrados en $\mathbb{Z}$.

Demostración: Si $p = a^2 + b^2$ en $\mathbb{Z}$ entonces $p = (a + b\cdot i)(a - b\cdot i)$ y como $N(a + b\cdot i) \neq 1$ se sigue que $p$ no es primo de Gauss (es sobrino!). Si recíprocamente $p$ no es primo de Gauss escribimos $p = z_1\cdot z_2$ en $\mathbb{Z}[i]$ con $N(z_1) \neq 1$ y $N(z_2) \neq 1$. Por lo tanto $p^2 = N(z_1)\cdot N(z_2)$. Pero siendo $p$ primo racional debe ser $p = N(z_1) = N(z_2)$. O sea, $p$ es suma de dos cuadrados enteros.

Los primos de Gauss son pues (salvo asociados) de los tres tipos siguientes:

I. Primos racionales $p > 0$ que no son suma de dos cuadrados en $\mathbb{Z}$.

II. Complejos $a + b\cdot i$, $a,b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ cuya norma es un primo racional impar.

III. El número complejo $1 + i$ de norma 2.

Próximamente veremos que los primos de la clase I son los primos racionales de la forma $4\cdot m + 3$ mientras que los complejos de II poseen norma igual a un primo racional de la forma $4\cdot m + 1$.

6.4. Ejercicios.

1. Probar que si $p$ es un primo racional que es suma de dos cuadrados en $\mathbb{Z}$ posee esencialmente una única forma de escribirse como suma de dos cuadrados en $\mathbb{Z}$ (lo de esencial se refiere a la posibilidad de cambiar el orden de los sumandos).
2. Probar que ningún primo racional de la forma $4m + 3$ puede escribirse como suma de dos cuadrados.

3. Sea $n = p_1 \cdots p_h$ donde cada $p_i$ es primo impar y todos son distintos entre sí.

   i. Probar que si cada $p_i$ es suma de dos cuadrados así lo es $n$.

   ii. Probar que si cada $p_i$ es suma de dos cuadrados entonces $n$ posee $2^{h-1}$ representaciones como suma de dos cuadrados del tipo $n = a^2 + b^2$, $0 < a < b$.

4. Sea $p$ primo impar. Sean $x,y \in \mathbb{N}$ con $2p = x^2 + y^2$. Probar que $p$ es suma de 2 cuadrados. (Sugerencia: $2p = (1 + i)(1 - i)p$).

6.5. Aplicación. Como nueva aplicación de la factorización única en $\mathbb{Z}[i]$ estudiaremos la representabilidad de enteros racionales como suma de dos cuadrados. Dado que todo entero $> 1$ es producto de primos y dado que todo producto de sumas de dos cuadrados es una suma de dos cuadrados, será suficiente analizar la representabilidad de números primos como suma de dos cuadrados. Este problema fue considerado y resuelto por Fermat en su famoso método del descenso.

6.6. TEOREMA. Sea $p$ un primo racional positivo e impar. Las afirmaciones son todas equivalentes entre sí:

i. La ecuación $x^2 \equiv -1 (\mathrm{mod}\ p)$ admite solución en $\mathbb{Z}$, o sea $-1$ es residuo cuadrático módulo $p$.

ii. $p \mid x^2 + 1$ para algún $x$ en $\mathbb{Z}$,

iii. $p$ no es primo de Gauss (amigo y gracias!)

iv. $p = x^2 + y^2$ para ciertos enteros $x,y$.

v. $p = 4m + 1$, para algún $m$ en $\mathbb{Z}$.

Demostración: i) $\Longrightarrow$ ii) es trivial.

ii) $\Rightarrow$ iii). Puesto que $x^2 + 1 = (x + i)\cdot(x - i)$ en $\mathbb{Z}[i]$, se tiene $p \mid x^2 + 1 \Rightarrow p \mid x + i$ ó $p \mid x - i$.

Sea $x + i = p\,z$ con $z$ en $\mathbb{Z}[i]$. Por conjugación resulta $x - i = p\cdot\bar{z}$ y sumando resulta $2x = p\cdot(z + \bar{z})$ en $\mathbb{Z}$. Por lo tanto $p = 2$ ó $p \mid x$.

La primera situación es imposible pues p es impar. Por otra $p \mid x \Rightarrow p \mid 1$, un absurdo. Concluimos que p no es primo en $\mathbb{Z}[i]$.

iii) $\Rightarrow$ iv). Escribamos en $\mathbb{Z}[i]$, una factorización propia de p: $p = (x_1 + y_1 \cdot i)\cdot(x_2 + y_2 \cdot i)$.

Tomando norma resulta $p^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2)$ en $\mathbb{Z}$ y como p es primo $p = x_1^2 + y_1^2 = x_2^2 + y_2^2$.

iv) $\Rightarrow$ v). Siendo p impar, se sigue de $p = x^2 + y^2$ que un sumando es par y el otro impar. Sea pues x par e y impar. Entonces $x^2 \equiv 0$ módulo 4 e $y^2 \equiv 1$ módulo 4, por lo tanto $p \equiv 1$ módulo 4.

v) $\Rightarrow$ ii). Sea $\mathbb{Z}_p$ el anillo de restos módulo p. Siendo p primo es bien sabido que $\mathbb{Z}_p$ es un cuerpo. Indiquemos con $\mathbb{Z}_p^*$ la totalidad de elementos de $\mathbb{Z}_p$ no nulos. Se sigue del teorema de Fermat que todo $x \in \mathbb{Z}_p^*$ satisface: $x^{p-1} = 1$ (o sea en $\mathbb{Z}$: $x^{p-1} \equiv 1$ módulo p si $p \nmid x$). Se tiene $x^{4m} = 1$, o sea $(x^{2m})^2 = 1$. Siendo p impar y $\mathbb{Z}_p$ un cuerpo la ecuación $x^2 = 1$ tiene dos soluciones únicas 1 y -1. Por lo tanto $x^{2m} = 1$ ó $x^{2m} = -1$.

Si algún x satisface $x^{2m} = -1$, resulta $(x^m)^2 = -1$ y nada queda por probar. Supongamos entonces que <u>todo</u> elemento de $\mathbb{Z}_p^*$ satisface $x^{2m} = 1$. Pero esto es un absurdo pues, otra vez, tratándose de un cuerpo, la ecuación $x^{2m} = 1$ tiene a lo sumo 2m soluciones en $\mathbb{Z}_p$ y $4m > 2m$. Hemos probado que v) $\Rightarrow$ ii). El teorema queda completamente demostrado.

6.7. COROLARIO. Las siguientes afirmaciones son equivalentes entre sí: Sea p primo racional positivo

i) $x^2 \equiv -1$ módulo p no admite solución en $\mathbb{Z}$

ii) p es primo en $\mathbb{Z}[i]$

iii) p <u>no</u> es suma de dos cuadrados en $\mathbb{Z}$

iv) $p = 4m + 3$ para algún $m \in \mathbb{Z}$.

<u>Demostración</u>: Se sigue por negación de las equivalencias en el Teorema.

6.8. COROLARIO. Sea $p$ primo impar. Entonces $p$ es de la forma $4m + 3$ sí y sólo si satisface la condición:

$$p \mid x^2 + y^2 \quad \text{en } \mathbb{Z} \Rightarrow p \mid x \quad y \quad p \mid y .$$

Demostración: Ejercicio para el lector.

6.9. COROLARIO. Sea $n = \Pi_i p_i^{e_i} \in \mathbf{N}$, con $p_i$ primos, $p_i \neq p_j$ si $i \neq j$. Entonces $n$ es suma de dos cuadrados sí y sólo si para todo índice $i$ tal que $p_i = 4m + 3$ el exponente $e_i$ es par.

6.10. Ejercicio. i) Hallar todas las soluciones de la ecuación $a^2 + b^2 = n!$, $a \leq b$, $n < 14$.

ii) Probar que la ecuación $y^2 = x^3 + 7$ no tiene soluciones enteras.

6.11. COROLARIO. Existen infinitos primos de la forma $4m + 3$ e infinitos primos de la forma $4\ell + 1$ con $m, \ell \in \mathbf{N}$.

Demostración: i) Sean $p_1, \ldots, p_s$ la totalidad de primos positivos de la forma $4m + 3$ con $p_i \neq 3$. Sea $t = \Pi p_i$ su producto. El número $4t + 3$ es impar, y distinto de 0 y 1. Es por lo tanto expresable como producto de primos en $\mathbb{Z}$.

Observemos ahora que el producto de enteros de la forma $4m + 1$ es otra vez de la forma $4n + 1$. Se sigue entonces que algún divisor primo de $4t + 3$ debe ser de la forma $4m + 3$. Pero debe ser distinto de 3, $p_1, \ldots, p_s$, un absurdo.

ii) Sean ahora $p_1, \ldots, p_s$ la totalidad de primos positivos de la forma $4m + 1$. Formemos el entero $4\cdot(p_1 \ldots p_s)^2 + 1$.

Dicho número es distinto de 0 y 1, por lo tanto admite algún divisor primo. La propiedad de los primos de la forma $4m + 3$ dada en el Corolario anterior, implica que los divisores primos de $h$ deben ser todos de la forma $4m + 1$. Pero debe ser alguno de los $p_1, \ldots, p_s$. Por lo tanto debe dividir a 1, un absurdo.

6.12. Suma de dos cuadrados.

Sea $p$ un primo racional positivo de la forma $4m + 1$. Entonces podemos escribir

$$p = a^2 + b^2 = (a + b\cdot i)\cdot(a - b\cdot i)$$

con $a$ y $b$ enteros positivos. Los enteros de Gauss $\pi_p := a + b\cdot i$, $\bar{\pi}_p := a - b\cdot i$ son primos de Gauss y entonces $p = \pi_p\cdot\bar{\pi}_p$ es la factorización de $p$ en $\mathbb{Z}[i]$. A manera de recapitulación se tiene que el comportamiento de los primos racionales en $\mathbb{Z}[i]$ es el siguiente. Denotemos con $q$ a los primos racionales positivos de la forma $4m + 3$ y con $p$ a los primos racionales positivos de la forma $4m + 1$. Entonces la factorización de un primo racional en producto de primos en $\mathbb{Z}[i]$ es asociada a una (y sólo una) de las siguientes $q$, $\pi_p\cdot\bar{\pi}_p$, $(1 + i)^2$. Por lo tanto todo entero racional $a \neq 0$ se factoriza en $\mathbb{Z}[i]$ como sigue

$$a = u\cdot(1 + i)^{a(2)}\cdot\Pi_q\, q^{a(q)}\cdot\Pi_p(\pi_p\cdot\bar{\pi}_p)^{a(p)}$$

con $a(2)$, $a(p)$, $a(q)$ enteros no negativos, $u := 1, -1, i, -i$, una unidad.

La factorización de $z \neq 0$, $z \in \mathbb{Z}[i]$ es del tipo siguiente

$$(1) \qquad z = u\cdot(1 + i)^{z(2)}\cdot\Pi_q\, q^{z(q)}\cdot\Pi_p(\pi_p^{z_1(p)}\cdot\bar{\pi}_p^{z_2(p)}).$$

6.13. Ejemplo. Hallemos la factorización prima de $33 + 44\cdot i$.

Dado que $33 + 44\cdot i = 11\cdot(3 + 4\cdot i)$, trabajamos primero con $3 + 4\cdot i$. tomando su norma resulta $N(3 + 4\cdot i) = 25 = 5\cdot 5 = (1 + 2\cdot i)^2(1 - 2\cdot i)^2$. Por lo tanto los posibles divisores primos de $3 + 4\cdot i$ son $1 + 2\cdot i$ ó $1 - 2\cdot i$ (o asociados). Por inspección resulta $3 + 4\cdot i = -1(1 - 2\cdot i)$. Por lo tanto resulta finalmente $33 + 44\cdot i = -1\cdot 11\cdot(1 - 2\cdot i)$ dado que 11 es primo de Gauss.

Veamos una aplicación de esa factorización. Sea $n \in \mathbb{N}$. Denotemos con $r_2(n)$ = cardinal de $\{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a^2 + b^2 = n\}$. Por ejemplo

$r_2(1) = 4$ , $r_2(2) = 4$ , $r_2(p) = 8$ , si $p > 0$ es primo de la forma $4m + 1$ , $r(q) = 0$ si $q > 0$ es primo de la forma $4m + 3$ , $r_2(6) = 0$ , $r_2(8) = 4$ . Es claro que $r_2(n)$ coincide con el cardinal de la totalidad de $z \in \mathbb{Z}[i]$ tales que $N(z) = n$ . Sea

$$(2) \qquad n = 2^{n(2)} \cdot \Pi_q \, q^{n(q)} \cdot \Pi_p \, p^{n(p)}$$

la factorización de $n$ en $\mathbb{Z}$ con las convenciones hechas más arriba sobre los primos $p$ y $q$ . Tomando norma en (1) e igualando con (2) resultan las identidades

$$n(2) = z(2)$$

$$n(q) = 2 \cdot z(q)$$

$$n(p) = z_1(p) + z_2(p) \, .$$

Se sigue que si $n(q)$ es impar para algún $q$ entonces $r_2(n) = 0$ . Las posibilidades para $z$ son entonces 4 valores distintos para las unidades $u$

$$z_1(p) = 0, 1, \ldots, n(p)$$

y $z_2(p)$ dependiendo de $z_1(p)$ por la condición $z_1(p) + z_2(p) = n(p)$ . En definitiva hay

$$4 \cdot \Pi_p (n(p) + 1) \qquad (p \text{ primo}, \; p = 4m + 1)$$

posibles elecciones de $z$ , tales que $N(z) = n$ .

En definitiva se tiene

$$r_2(n) = 0 \quad \text{si } n(q) \text{ es impar } (q \text{ primo} > 0 \, , \; q = 4m + 3)$$

$$r_2(n) = 4 \cdot \Pi_p (n(p) + 1) \quad \text{si } n(q) \text{ es par.}$$

El comportamiento de $\sum_{n \le x} r_2(n)$ es asintótico a la función $x \cdot \pi$ . En efecto, sobre el círculo de radio $\sqrt{x}$ , $x$ real positivo y de centro en $(0,0) \in R^2$ , el número de $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ que yacen sobre el mismo es

$$\sum_{n \leq x} r_2(n)$$

En efecto, notar que $n = a^2 + b^2 \leq x \Leftrightarrow (a,b) \in$ círculo de radio $\sqrt{x}$. Si a cada punto $(a,b)$ de coordenadas enteras le asociamos el cuadrado de área 1 cuyo vértice superior derecho es $(a,b)$ es claro que la suma anterior aproxima el área del círculo o sea el valor $\pi \cdot x$, por lo tanto

$$\frac{\sum_{n \leq x} r_2(n)}{x \cdot \pi} \to 1 \quad \text{cuando} \quad x \to \infty$$

o también

$$\lim_{x \to \infty} \frac{\sum_{n \leq x} r_2(n)}{x} = \pi .$$

6.14. Ejercicios.

1. Hallar todos los $z \in Q(i)$ tales que $N(z) = 1$.
2. Hallar cuociente y resto de la división de $2 + i$ por $i$, $2 + 3i$ por $1 + i$, $3 - 2i$ por $1 + 2i$, $1 + i$ por $1 - i$.
3. Determinar cuáles de los siguientes enteros de Gauss son primos: $1 + 4i$, $7 + 13i$, $1 + 3i$, $9 + 4i$, $1 + 10i$, $3 + 7i$.
4. Hallar todos los $z,w$ en $\mathbb{Z}[i]$ tales que $5 - i = (1 + 2i)w + z$ con $N(z) < N(1 + 2i)$.
5. Hallar el mcd en $\mathbb{Z}[i]$ de: $15 + 21i$ y $3 - 9i$. Lo mismo para $3 + 8i$ y $12 + i$.
6. Resolver las siguientes ecuaciones de congruencias: $(1 + i)X \equiv 1 \pmod 3$ $(2 + i)X \equiv 3 - i \pmod{1 + 4i}$.
7. ¿Pueden los enteros siguientes: 390, 306, 665 ser longitudes de hipotenusas de triángulos rectángulos con catetos enteros?
8. Resolver las ecuaciones diofantinas: $X^2 + 1 = y^2$, $X^2 + 4 = y^3$, $X^2 + 11 = Y^3$, $X^2 + Y^2 = 2Z^2$.
9. Hallar una familia infinita de soluciones de la ecuación $X^2 + Y^2 = Z^3$.
10. Sea $n$ natural. Probar que si $n$ es suma de dos cuadrados en $Q$ también lo es en $\mathbb{N}$.

# TABLA DE DESCOMPOSICION DE PRIMOS DE LA FORMA 4n + 1 EN SUMA DE DOS CUADRADOS.



I. Tabelle* für die Zerfällung der Primzahlen $p$ von der Form $4n+1$ in die Summe zweier Quadrate *).

$$p = a^2 + b^2.$$

| $p$ | $a$ | $b$ | $p$ | $a$ | $b$ | $p$ | $a$ | $b$ | $p$ | $a$ | $b$ | $p$ | $a$ | $b$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 1 | 2 | 401 | 1 | 20 | 881 | 15 | 16 | 1409 | 35 | 18 | 1993 | 43 | 18 | 2549 | 7 | 50 |
| 17 | 1 | 4 | 409 | 3 | 20 | 929 | 13 | 20 | 1429 | 13 | 30 | 1997 | 19 | 34 | 2557 | 11 | 46 |
| 29 | 5 | 2 | 421 | 15 | 14 | 937 | 19 | 24 | 1433 | 37 | 8 | 2017 | 9 | 44 | 2593 | 37 | 28 |
| 37 | 1 | 6 | 433 | 17 | 12 | 941 | 19 | 10 | 1453 | 3 | 38 | 2029 | 45 | 2 | 2609 | 47 | 30 |
| 41 | 5 | 4 | 449 | 7 | 20 | 953 | 13 | 28 | 1481 | 35 | 16 | 2053 | 27 | 40 | 2617 | 51 | 4 |
| 53 | 7 | 2 | 457 | 21 | 4 | 977 | 31 | 4 | 1489 | 33 | 20 | 2069 | 25 | 38 | 2621 | 11 | 50 |
| 61 | 5 | 6 | 461 | 19 | 10 | 997 | 31 | 6 | 1493 | 7 | 38 | 2081 | 41 | 20 | 2633 | 43 | 18 |
| 73 | 3 | 8 | 509 | 5 | 22 | 1009 | 15 | 28 | 1549 | 35 | 12 | 2089 | 45 | 8 | 2657 | 49 | 16 |
| 89 | 5 | 8 | 521 | 11 | 20 | 1013 | 31 | 12 | 1553 | 33 | 22 | 2113 | 33 | 32 | 2677 | 35 | 34 |
| 97 | 9 | 4 | 541 | 21 | 10 | 1021 | 11 | 30 | 1597 | 31 | 24 | 2129 | 23 | 40 | 2689 | 33 | 40 |
| 101 | 1 | 10 | 557 | 19 | 14 | 1033 | 3 | 32 | 1601 | 1 | 40 | 2137 | 29 | 36 | 2693 | 47 | 22 |
| 109 | 3 | 10 | 569 | 13 | 20 | 1049 | 5 | 32 | 1609 | 3 | 40 | 2141 | 5 | 46 | 2713 | 3 | 52 |
| 113 | 7 | 8 | 577 | 1 | 24 | 1061 | 31 | 10 | 1613 | 13 | 36 | 2153 | 37 | 28 | 2729 | 5 | 52 |
| 137 | 11 | 4 | 593 | 23 | 8 | 1069 | 13 | 30 | 1621 | 39 | 10 | 2161 | 15 | 44 | 2741 | 23 | 46 |
| 149 | 7 | 10 | 601 | 5 | 24 | 1093 | 33 | 2 | 1637 | 31 | 26 | 2213 | 47 | 2 | 2749 | 43 | 30 |
| 157 | 11 | 6 | 613 | 17 | 18 | 1097 | 19 | 26 | 1657 | 19 | 38 | 2221 | 45 | 14 | 2753 | 7 | 52 |
| 173 | 13 | 2 | 617 | 19 | 16 | 1109 | 33 | 20 | 1669 | 13 | 38 | 2237 | 21 | 46 | 2777 | 19 | 44 |
| 181 | 9 | 10 | 641 | 25 | 4 | 1117 | 31 | 16 | 1693 | 37 | 18 | 2269 | 37 | 30 | 2789 | 17 | 50 |
| 193 | 7 | 12 | 653 | 23 | 22 | 1129 | 27 | 20 | 1697 | 41 | 4 | 2273 | 47 | 8 | 2797 | 31 | 44 |
| 197 | 1 | 14 | 661 | 25 | 6 | 1153 | 33 | 8 | 1709 | 35 | 22 | 2281 | 45 | 16 | 2801 | 49 | 10 |
| 229 | 15 | 2 | 673 | 23 | 22 | 1181 | 3 | 34 | 1721 | 11 | 40 | 2293 | 13 | 42 | 2833 | 13 | 48 |
| 233 | 13 | 8 | 677 | 1 | 26 | 1193 | 15 | 32 | 1733 | 17 | 38 | 2297 | 19 | 44 | 2837 | 41 | 34 |
| 241 | 15 | 4 | 701 | 5 | 26 | 1201 | 25 | 24 | 1741 | 29 | 30 | 2309 | 47 | 10 | 2857 | 31 | 36 |
| 257 | 1 | 16 | 709 | 25 | 20 | 1213 | 27 | 22 | 1753 | 27 | 32 | 2333 | 43 | 30 | 2861 | 29 | 50 |
| 269 | 13 | 10 | 733 | 27 | 2 | 1217 | 31 | 16 | 1777 | 39 | 16 | 2341 | 13 | 46 | 2897 | 31 | 44 |
| 277 | 9 | 14 | 757 | 9 | 26 | 1229 | 35 | 2 | 1789 | 5 | 42 | 2357 | 41 | 28 | 2909 | 53 | 10 |
| 281 | 5 | 16 | 761 | 25 | 20 | 1237 | 9 | 34 | 1801 | 35 | 24 | 2377 | 35 | 34 | 2917 | 1 | 54 |
| 293 | 17 | 6 | 769 | 25 | 12 | 1249 | 15 | 32 | 1861 | 31 | 30 | 2381 | 35 | 34 | 2953 | 43 | 36 |
| 313 | 13 | 12 | 773 | 27 | 22 | 1277 | 21 | 34 | 1873 | 33 | 32 | 2389 | 25 | 44 | 2957 | 19 | 46 |
| 317 | 11 | 14 | 797 | 11 | 26 | 1289 | 35 | 8 | 1877 | 41 | 14 | 2393 | 37 | 32 | 2969 | 37 | 40 |
| 337 | 9 | 16 | 809 | 5 | 28 | 1297 | 9 | 36 | 1889 | 17 | 40 | 2417 | 49 | 4 | 3001 | 51 | 10 |
| 349 | 5 | 18 | 821 | 25 | 14 | 1301 | 25 | 26 | 1901 | 35 | 26 | 2437 | 49 | 6 | 3037 | 11 | 54 |
| 353 | 17 | 8 | 829 | 27 | 10 | 1321 | 5 | 36 | 1913 | 23 | 36 | 2441 | 35 | 38 | 3041 | 35 | 4 |
| 373 | 7 | 18 | 853 | 23 | 18 | 1361 | 31 | 10 | 1933 | 13 | 42 | 2473 | 13 | 48 | 3049 | 43 | 32 |
| 389 | 17 | 10 | 857 | 29 | 4 | 1373 | 37 | 2 | 1949 | 43 | 10 | 2477 | 19 | 46 | 3061 | 55 | 6 |
| 397 | 19 | 6 | 877 | 29 | 6 | 1381 | 15 | 34 | 1973 | 13 | 38 | 2521 | 35 | 36 | 3089 | 53 | 8 |

*) Ich lasse hier die Tabellen folgen, die ich in dem vorstehenden Aufsatze erwähnt habe. Die Berechnung der Tabellen I und II verdanke ich der Gefälligkeit des Herrn Director Zornow. Oct. 1845.

*Siehe S. 428.

7. EL ANILLO $\mathbb{Z}[\sqrt{-5}]$ .

Es éste un dominio carente de factorización única en producto de elementos irreductibles. Veremos que todo elemento en $\mathbb{Z}[\sqrt{-5}]$ posee descomposición en producto de irreductibles pero no necesariamente en forma única. $\mathbb{Z}[\sqrt{-5}]$ es, como dijimos anteriormente, la totalidad de números complejos de la forma $a + b\sqrt{-5}$ con $a$ y $b$ enteros y denotando $\sqrt{-5}$ un número complejo (fijo) cuyo cuadrado es $-5$ . Es un ejercicio sencillo probar que $\mathbb{Z}[\sqrt{-5}]$ es efectivamente un anillo. El cuerpo de cuocientes de $\mathbb{Z}[\sqrt{-5}]$ se denota por $\mathbb{Q}(\sqrt{-5})$ y consiste de la totalidad de números complejos de la forma $r + s\sqrt{-5}$ con $r$ y $s$ números racionales (una verificación es necesaria!). Para el estudio de $\mathbb{Z}[\sqrt{-5}]$ , al igual que en $\mathbb{Z}[i]$ es útil introducir la llamada norma. Sea pues $z = a + b\sqrt{-5}$ . Se define el conjugado de $z$ en $\mathbb{Q}(\sqrt{-5})$ por

$$\bar{z} = a - b\sqrt{-5}$$

y la norma $N(z)$ de $z$ por $N(z) = z\cdot\bar{z}$ .

Notar que $N(a + b\sqrt{-5}) = a^2 + 5\cdot b^2$

Se satisfacen las siguientes propiedades:

i) $N(z) \geq 0$

ii) $N(z) = 0$ si y sólo si $z = 0$ .

iii) $N(z_1\cdot z_2) = N(z_1)\cdot N(z_2)$ .

La propiedad iii) dice que el producto de dos enteros o racionales de la forma $a^2 + 5\cdot b^2$ es también de esa forma!

7.1. Falla del Lema de Aproximación.

En 3.1 vimos la validez de un lema de aproximación de elementos de $\mathbb{Q}(i)$ por enteros de Gauss. Este Lema nos permitió probar la existencia de un algoritmo de división en $\mathbb{Z}[i]$ . Veamos que esta situación no se dá en $\mathbb{Z}[\sqrt{-5}]$ . Sea $z = 1/2 + 1/2\sqrt{-5} \in \mathbb{Q}(\sqrt{-5})$ . Entonces si $q = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ se tiene

$$N(z - q) = (a - 1/2)^2 + 5(b - 1/2)^2 = 1/4(2a - 1)^2 +$$

$$+ 5/4(2b - 1)^2 > 5/4(2b - 1)^2 > 5/4 > 1 .$$

La existencia de algoritmo de división por esta vía queda bloqueada. En realidad no existe un $\mathbb{Z}[\sqrt{-5}]$ ningún algoritmo de división simplemente pues $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única!

7.2. Unidades en $\mathbb{Z}[\sqrt{-5}]$ .

Es claro que $u \in U\mathbb{Z}[\sqrt{-5}]$ sí y sólo si $N(u) = 1$ . (Demostrar!)

Por lo tanto hay que hallar todas las soluciones de la ecuación

$a^2 + 5 \cdot b^2 = 1$ .

Es claro que las únicas posibilidades son $a = 1$ ó $a = -1$ , o sea, 1 y -1 son todas las unidades de $\mathbb{Z}[\sqrt{-5}]$ .

7.3. Ejemplo.

3 es irreductible en $\mathbb{Z}[\sqrt{-5}]$ , pero no es primo en $\mathbb{Z}[\sqrt{-5}]$ . En efecto,

$3 = z_1 \cdot z_2$ en $\mathbb{Z}[\sqrt{-5}]$ (tomando norma)

$9 = N(z_1) \cdot N(z_2)$ en $\mathbb{Z}$ .

Siendo 3 primo en $\mathbb{Z}$ se debe verificar $N(z_1)$ ó $N(z_2)$ es 1 , es decir $z_1$ ó $z_2$ es unidad en $\mathbb{Z}[\sqrt{-5}]$ por lo tanto la factorización dada es impropia. Ver que 3 no es primo queda como ejercicio.

7.4. Ejemplo. 11 es primo en $\mathbb{Z}[\sqrt{-5}]$ .

En efecto, sean $z_1, z_2, w$ en $\mathbb{Z}[\sqrt{-5}]$ tales que $z_1 \cdot z_2 = 11 \cdot w$ en $\mathbb{Z}[\sqrt{-5}]$ . Es decir, 11 divide al producto $z_1 \cdot z_2$ . Tomando norma resulta

$$N(z_1) \cdot N(z_2) = 11^2 \cdot N(w) \quad \text{en } \mathbb{Z} .$$

Por lo tanto $N(z_1)$ (digamos) es divisible por 11. Se tiene entonces si $N(z_1) = a^2 + 5 \cdot b^2$ , $a^2 + 5 \cdot b^2 \equiv 0 (\text{mod } 11)$ .

Dejamos a cargo del lector probar que se sigue de esa congruencia que a y b son divisibles por 11, por lo tanto 11 divide a $z_1$ .

Q.E.D.

7.5. Ejemplo. $41$ no es irreductible en $\mathbb{Z}[\sqrt{-5}]$ . En efecto, $41 = 6^2 + 5\cdot 1 = (6 + \sqrt{-5})\cdot(6 - \sqrt{-5})$ . El primo racional 29 no es irreductible en $\mathbb{Z}[\sqrt{-5}]$ pues $29 = 3^2 + 5\cdot 2^2 = (3 + 2\sqrt{-5})\cdot(3 - 2\sqrt{-5})$ .

7.6. $\mathbb{Z}[\sqrt{-5}]$ no es un DFU.

En efecto, mostremos que $9 = 3\cdot 3 = (2 + \sqrt{-5})\cdot(2 - \sqrt{-5})$ son factorizaciones esencialmente diferentes en producto de irreductibles. Sabemos que 3 es irreductible. Análogamente ocurre con $2 + \sqrt{-5}$ y $2 - \sqrt{-5}$ utilizando el mismo razonamiento.

Nos quedaría por ver que 3 no es asociado de $2 + \sqrt{-5}$ , ni de $2 - \sqrt{-5}$ . Pero esto es trivialmente cierto dado que las únicas unidades de $\mathbb{Z}[\sqrt{-5}]$ son 1 y -1. La afirmación queda probada.

Mostremos que todo elemento $z$ en $\mathbb{Z}[\sqrt{-5}]$ , $z \neq 0,1,-1$ es producto de irreductibles. Si $z$ no es irreductible es producto de factores $z = z_1 \cdots z_r$ con $z_i \neq 1,-1$ . Por lo tanto $N(z_i) \geq 2$ y entonces $N(z) = N(z_1) \cdots N(z_r) \geq 2^r$ con lo que $r$ está acotado. Por lo tanto el lector puede convencerse que $z$ admite una factorización en producto de irreductibles.

7.7. Comportamiento de los primos racionales dentro de $\mathbb{Z}[\sqrt{-5}]$ .

En los ejemplos vimos que el primo racional 3 deja de ser primo en $\mathbb{Z}[\sqrt{-5}]$ , mientras que 11 sigue siendo primo.

El primo 5 tiene un comportamiento particular: $5 = -1\,(\sqrt{-5})^2$ , y es fácil ver que $\sqrt{-5}$ es irreductible. Se dice que 5 se ramifica en $\mathbb{Z}[\sqrt{-5}]$ . Es el único primo racional con la propiedad de ser asociado en $\mathbb{Z}[\sqrt{-5}]$ , a un cuadrado.

Introduzcamos el símbolo de Legendre. Sea $p$ primo impar. Se define para todo $a \in \mathbb{Z}$ :

$\left(\frac{a}{p}\right) = 1$ si $a$ es residuo cuadrático módulo $p$ .

$\left(\frac{a}{p}\right) = 0$ si $p \mid a$

$\left(\frac{a}{p}\right) = -1$ si $a$ no es residuo cuadrático módulo $p$ .

7.8. TEOREMA. Sea $p$ primo racional impar. Entonces

$$\left(\frac{-5}{p}\right) = -1 \longrightarrow p \text{ es primo en } \mathbb{Z}[\sqrt{-5}] .$$

Demostración: Sea $\left(\frac{-5}{p}\right) = 1$. Es decir $-5$ es residuo cuadrático módulo $p$. Significa que $-5$ es un cuadrado módulo $p$ : $-5 \equiv a^2 + p\cdot x$ con $a,x$ en $\mathbb{Z}$. Se tiene

$$p\cdot(-x) = a^2 + 1\cdot 5 = (a + \sqrt{-5})\cdot(a - \sqrt{-5}) .$$

Si fuera $p$ primo entonces podríamos escribir, por ejemplo:

$$a + \sqrt{-5} = p\cdot w \quad \text{con} \quad w \in \mathbb{Z}[\sqrt{-5}]$$

y por conjugación también

$$a - \sqrt{-5} = p\cdot\bar{w} .$$

Sumando ambas expresiones y usando el hecho que $p$ es impar y $w + \bar{w} \in \mathbb{Z}$, resulta que $p$ divide a $a$ en $\mathbb{Z}$. Pero entonces $p$ divide a 5 por una igualdad de más arriba, o sea $\left(\frac{-5}{p}\right) = 0$, un absurdo.

Sea $\left(\frac{-5}{p}\right) = -1$. Sean $z_1, z_2$ en $\mathbb{Z}[\sqrt{-5}]$ tales que $p \mid z_1\cdot z_2$. Tomando norma resulta $p \mid N(z_1)\cdot N(z_2)$. Supongamos $p \mid N(z_1)$, $z_1 = a + b\sqrt{-5}$. Entonces $a^2 + 5b^2 \equiv 0 (\text{mod } p)$. Si $b \not\equiv 0 (\text{mod } p)$ entonces $\left(\frac{-5}{p}\right) = 1$. Por lo tanto $p \mid b$ y así $p \mid a$, con lo que $p \mid z_1$. El teorema queda pues demostrado.

Se sigue que 11, 13, 17, 19 son primos en $\mathbb{Z}[\sqrt{-5}]$ pero no lo son 3, 7, 23.

El comportamiento de 2 es el siguiente; 2 es irreductible pero no primo: 2 divide al producto $(1 + \sqrt{-5})\cdot(1 - \sqrt{-5})$ pero no divide a ninguno de los factores (por el argumento corriente de tomar norma!)

7.9. COROLARIO. Sea $p$ primo racional. Supongamos $\left(\frac{-5}{p}\right) = -1$. Entonces en $\mathbb{Z}$, $p \mid a^2 + 5b^2 \Rightarrow p \mid a$ y $p \mid b$.

Demostración: Si $p \mid b$ entonces $a^2 + 5b^2 \equiv 0 (\text{mod } p) \Rightarrow -5$ es cuadrado módulo $p$, por lo tanto $p \mid b$ y así $p \mid a$.

7.10. Introducción de factores primos ideales.

Sea $A = \mathbb{Z}[\sqrt{-5}]$ y sean las factorizaciones de 21:

$$21 = 3\cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5}) .$$

Se trata de estudiar la posibilidad de introducir factores primos ideales tales como $3 = \alpha_1\cdot\alpha_2$ , $7 = \beta_1\cdot\beta_2$ de manera de recomponer la factorización única por simple asociación de los factores. Supongamos que

$$\alpha_1 \mid 1 + 2\sqrt{-5} \qquad \alpha_2 \mid 1 - 2\sqrt{-5}$$

$$\beta_1 \mid 1 + 2\sqrt{-5} \qquad \beta_2 \mid 1 - 2\sqrt{-5} .$$

La definición de estos factores ideales estará obviamente ligada a la propiedad de divisibilidad. Por ejemplo tratemos de interpretar $\alpha_1 \mid z$ , $z \in A$ , $z = x + y\sqrt{-5}$ .

Se tendrá $z = \alpha_1\cdot\delta$ , para algún factor (ideal) $\delta$ . Ahora dado que $\alpha_1 \mid 1 + 2\sqrt{-5}$ , se deberá verificar que

$$(1 - 2\sqrt{-5})\cdot z = (1 - 2\sqrt{-5})\cdot\alpha_1\cdot\delta \equiv 0 (\mathrm{mod}\ 3) .$$

Recíprocamente si $3 \mid (1 - 2\sqrt{-5})\cdot z$ entonces como $3 = \alpha_1\cdot\alpha_2$ y $\alpha_2 \mid 1 - 2\sqrt{-5}$ , se tendrá $\alpha_1 \mid z$ . Por lo tanto decretaremos

$$\alpha_1 \mid z \rightarrow (1 - 2\sqrt{-5})\cdot z \equiv 0 (\mathrm{mod}\ 3) .$$

Análogamente,

$$\alpha_2 \mid z \rightarrow (1 + 2\sqrt{-5})\cdot z \equiv 0 (\mathrm{mod}\ 3)$$

$$\beta_1 \mid z \rightarrow (1 - 2\sqrt{-5})\cdot z \equiv 0 (\mathrm{mod}\ 7)$$

$$\beta_2 \mid z \rightarrow (1 + 2\sqrt{-5})\cdot z \equiv 0 (\mathrm{mod}\ 7) .$$

Se sigue que si $z = x + y\sqrt{-5}$ ,

$$(1 - 2\sqrt{-5})\cdot z = (x + 10y) + (y - 2x)\sqrt{-5}$$

$$(1 + 2\sqrt{-5})\cdot z = (x - 10y) + (y + 2x)\sqrt{-5}$$

y por lo tanto

$\alpha_1 \mid z \longrightarrow x + y \equiv 0 (\text{mod } 3)$

$\alpha_2 \mid z \longrightarrow x - y \equiv 0 (\text{mod } 3)$

$\beta_1 \mid z \longrightarrow x + 3y \equiv 0 (\text{mod } 7)$

$\beta_2 \mid z \longrightarrow x - 3y \equiv 0 (\text{mod } 7)$ .

Veamos el comportamiento de estos factores respecto de productos. Sean $z = x + y\sqrt{-5}$ , $z_1 = x_1 + y_1\sqrt{-5}$ . Entonces

$$\alpha_1 \mid z \cdot z_1 \longrightarrow xx_1 - 5yy_1 + xy_1 + yx_1 \equiv 0 (\text{mod } 3)$$

$$\longrightarrow xx_1 + yy_1 + xy_1 + yx_1 \equiv 0 (\text{mod } 3)$$

$$\longrightarrow (x + y)(x_1 + y_1) \equiv 0 (\text{mod } 3)$$

$$\longrightarrow (x + y \equiv 0 \text{ ó } x_1 + y_1 \equiv 0 (\text{mod } 3)$$

$$\longrightarrow \alpha_1 \mid z \text{ ó } \alpha_1 \mid z_1 ,$$

de manera que $\alpha_1$ es un factor primo, en sentido de la divisibilidad. Lo mismo se verifica con $\alpha_2$, $\beta_1$, $\beta_2$ . Repasando la factorización de 21 se tiene $21 = \alpha_1 \cdot \alpha_2 \cdot \beta_1 \cdot \beta_2$ , y además

$\alpha_2 \mid 4 + \sqrt{-5}$ $\qquad$ $\beta_1 \mid 4 + \sqrt{-5}$

$\alpha_1 \mid 4 - \sqrt{-5}$ $\qquad$ $\beta_2 \mid 4 - \sqrt{-5}$

$\alpha_1 \mid 1 + 2\sqrt{-5}$ $\qquad$ $\beta_1 \mid 1 + 2\sqrt{-5}$

$\alpha_2 \mid 1 - 2\sqrt{-5}$ $\qquad$ $\beta_2 \mid 1 - 2\sqrt{-5}$ ,

por lo tanto $3 \cdot 7 = (\alpha_1\alpha_2)(\beta_1\beta_2)$

$$(1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (\alpha_1\beta_1)(\alpha_2\beta_2)$$

$$(4 + \sqrt{-5})(4 - \sqrt{-5}) = (\alpha_2\beta_1)(\alpha_1\beta_2) .$$

La factorización en producto de factores primos ideales queda restablecida.

Ejemplo: $9 = 3 \cdot 3 = \alpha_1^2 \cdot \alpha_2^2$

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}) .$$

Dado que $\alpha_1 \mid 2 + \sqrt{-5}$ , $\alpha_1 \mid 2 - \sqrt{-5}$ se sigue que

$$2 + \sqrt{-5} = \alpha_1^2$$

$$2 - \sqrt{-5} = \alpha_2^2$$

de manera que el cuadrado del factor ideal $\alpha_1$ (y lo mismo de $\alpha_2$) es "real" o sea es un elemento de $\mathbb{Z}[\sqrt{-5}]$ . De la teoría de Kummer se sigue que para todo factor ideal $\alpha$ es $\alpha^2$ un factor real, o sea un elemento de $\mathbb{Z}[\sqrt{-5}]$ .

En el desarrollo general de números ideales Kummer descubrió que para ciertos dominios numéricos existe un número natural denotado universalmente por $h$ , llamado el número de clases con la propiedad que, para todo factor ideal $\alpha$ se verifica que $\alpha^h$ es un factor "real" o sea un elemento del dominio. Para $\mathbb{Z}[\sqrt{-5}]$ este número es precisamente 2. Para $\mathbb{Z}[i]$ este número es 1, debido a que en este dominio no hace falta introducir factores ideales, pues $\mathbb{Z}[i]$ es un dominio de factorización única. Fué Richard Dedekind quien retomó la obra de Kummer y generalizó sus ideas para desarrollar una teoría general de números algebraicos que publicó en el famoso Suplemento del libro de Dirichlet: Vorlesungen über Zahlentheorie (1863). Uno de los logros esenciales de Dedekind fue dar "realidad" a los factores ideales de Kummer. Veamos esto para nuestra situación particular de $\mathbb{Z}[\sqrt{-5}]$ . Consideremos el factor ideal $\alpha_1$. Hemos visto que si $z = x + y\sqrt{-5}$ entonces $\alpha_1 \mid z \rightarrow x + y \equiv 0 (\mathrm{mod}\ 3)$ . O sea, $\alpha_1 \mid z$ sí y sólo si para algún entero $k$ ,

$$z = y + 3k + y\sqrt{-5} = 3k + (-1 + \sqrt{-5})y .$$

Por lo tanto si denotamos con $(3, -1 + \sqrt{-5})$ la totalidad de combinaciones con coeficientes en $\mathbb{Z}$

$$3k + (-1 + \sqrt{-5})y$$

se tiene que $(3,-1+\sqrt{-5}) = (z \in \mathbb{Z}[\sqrt{-5}] \mid \alpha_1 \mid z)$ .

Siguiendo su clásica definición de número real como subconjunto de números racionales, Dedekind define el factor ideal $I = \alpha_1 := (3,-1+\sqrt{-5})$

El subconjunto I tiene las propiedades

$$a,b \in I \Rightarrow a + b \in I$$

$$a \in I\ ,\quad b \in A \Rightarrow a\cdot b \in I \qquad 0 \in I\ .$$

O sea I es un ideal como lo llamara Dedekind y como se estudia hoy en cualquier curso de Algebra II. Todo elemento $z \in A$ define un ideal, a saber la totalidad, designada por $(z)$ , de todos los múltiplos de z en A : $(z) = (k\cdot z \mid k \in A)$.

La teoría de la divisibilidad se realiza ahora en términos ideales y el hecho fundamental de la teoría de Dedekind es que en dominios numéricos vale un teorema fundamental de la Aritmética relativo a la factorización única de ideales en producto de ideales primos. Los restantes factores ideales $\alpha_2, \beta_1, \beta_2$ se traducen en los ideales: $\alpha_2 = (3,1+\sqrt{-5})$ , $\beta_1 = (7,-3+\sqrt{-5}) = (7,4+\sqrt{-5})$ , $\beta_2 = (7,3+\sqrt{-5})$ .

8. Ideales. Sea A un anillo conmutativo con elemento neutro $1 \neq 0$ . Un ideal en A es todo subconjunto no vacío I con las propiedades siguientes:

$$x,y \in I \Rightarrow x - y \in I$$

$$y \in I\ ,\quad x \in A \Rightarrow y\cdot x \in I$$

o sea I es cerrado respecto a la suma y producto por elementos de A . Se sigue de la definición que para todo ideal I de A : $0 \in I$ , $y \in I \Rightarrow -y \in I$ .

El ejemplo más simple de ideal resulta de tomar un elemento $a \in A$ y formar la totalidad de múltiplos de a en A . Escribimos

$$(a) := (x\cdot a \mid x \in A)\ .$$

Más generalmente podemos tomar una familia finita $a_1, a_2, \ldots, a_m$ de elementos de $A$ y formar la totalidad de combinaciones lineales

$$x_1 \cdot a_1 + x_2 \cdot a_2 + \ldots + x_m \cdot a_m$$

con coeficientes $x_i \in A$. Es sencillo verificar que obtenemos un ideal en $A$ que denotamos con $(a_1, \ldots, a_n)$.

Decimos que es el ideal generado por $a_1, \ldots, a_n$.

En el caso $(a)$ decimos que es un ideal principal.

El anillo $A$ se dice a ideales principales si todo ideal es principal.

Notar que $0 := (0)$, $A = (1)$, son ideales que denominamos triviales.

Dejamos a cargo del lector probar que $A$ es un cuerpo (o sea, todo elemento no nulo es inversible) sí y sólo si $A$ posee dos únicos ideales (... los triviales).

Ejercicios:

i. Probar que en $\mathbb{Z}$ todo ideal es principal.

ii. Probar que en $\mathbb{Z}$, $(a) \subset (b) \Leftrightarrow b \mid a$.

iii. Sean $a$ y $b \in A$. Probar que $(a) = (b)$ sí y sólo si existe $u \in U(A)$ tal que $a = u \cdot b$.

iv. Sea $I$ un ideal de $A$. Probar que $I = A$ sí y sólo si $\phi \neq U(A) \cap A$.

v. Sea $K$ un cuerpo y sea $A = K[X]$. Probar que todo ideal de $K[X]$, es principal.

vi. Sea $A = \mathbb{Z}[X]$ el anillo de polinomios con coeficientes enteros y sea $I$ la totalidad de polinomios en $\mathbb{Z}[X]$ de la forma: $a_n X^n + \ldots + a_1 X + a_0$, con $a_0$ entero par. Probar que $I$ es un ideal de $A$ que no es principal. Probar que $I = (2, X)$.

vii. Sean $A$ y $A'$ anillos conmutativos con identidad. Un morfismo de $A$ en $A'$ es toda aplicación $f : A \to A'$ que satisface

$$f(x + y) = f(x) + f(y)$$

$$f(x \cdot y) = f(x) \cdot f(y)$$

$$f(1) = 1$$

$x,y \in A$ , 1 denota ambas identidades.

- Probar que $Nu(f) = \{x \mid x \in A , f(x) = 0\}$ (Núcleo de f) es un ideal de A .
- Probar que f es inyectivo sí y sólo si $Nu(f) = 0$ .

Sea para cada $n \in \mathbb{N}$, $\mathbb{Z}_n$ : el anillo de restos módulo n .

- Probar que $f : \mathbb{Z} \to \mathbb{Z}_n$ definido por $f(a) =$ resto de a en la división por n y que denotamos $\tilde{a}$ , es un morfismo sobre, cuyo núcleo es el ideal $(n)$ de múltiplos de n .
- Probar que $\mathbb{Z}_n$ es un anillo principal.
- Probar que $\mathbb{Z}_n$ es un cuerpo sí y sólo si n es un número primo.

Un ideal P en A se dice primo si satisface las condiciones:

p1) $P \neq A$

p2) $x,y \in A , x \cdot y \in P \Rightarrow x \in P$ ó $y \in P$ .

Ejercicios.

i. Probar que en $\mathbb{Z}$, un ideal P es primo sí y sólo si $P = 0$ ó $P = (p)$ , con p primo.

ii. Probar que un anillo A es un dominio (o sea $x \cdot y = 0$ en $A \Rightarrow x = 0$ ó $y = 0$) sí y sólo si 0 es ideal primo.

iii. Sea A un dominio de factorización única. Probar que un elemento $a \in A$ es primo (o sea $p \mid x \cdot y$ en A sí y sólo si $p \mid x$ ó $p \mid y$) sí y sólo si el ideal $(p)$ es primo.

iv. Sea A un dominio principal. Probar que todo ideal primo es maximal (es decir no existe ningún ideal $I \neq A$ que lo contenga propiamente).

Anillo cuociente. Sea A un anillo conmutativo y sea I un ideal de A . Para cada $a \in A$ denotamos con $\tilde{a}$ al subconjunto de A :

$$\tilde{a} = a + I$$

o sea la totalidad de elementos de A que son suma de a y un elemento cualquiera de A . Notar que $\tilde{a} = I \Leftrightarrow a \in I$ .

Es útil pensar que $\bar{a}$ es el "trasladado" de $I$ por $a$. Denotaremos por $A/I$ la totalidad de esos subconjuntos que llamaremos clases según $I$. Estas clases no son otra cosa que las clases de equivalencia de la relación de equivalencia en $A$: $x \sim y \Leftrightarrow x - y \in I$.
La aplicación $f : A \to A/I$ definida por $f(a) = \bar{a}$, la llamaremos, aplicación canónica.

Ejemplo. Sea $A = \mathbb{Z}$ y sea $I = (n)$. Entonces $\mathbb{Z}/(n)$ consta de las clases:

$$\bar{0} = \{k \cdot n \mid k \in \mathbb{Z}\}$$
$$\bar{1} = \{k \cdot n + 1 \mid k \in \mathbb{Z}\}$$
$$\ldots$$
$$\overline{(n-1)} = \{k \cdot n + (n-1) \mid k \in \mathbb{Z}\}.$$

Si $n = 3$ se tienen las clases

$$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$\bar{1} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$\bar{2} = \{\ldots, -4, -1, 1, 2, 5, 8, \ldots\}.$$

El conjunto $A/I$ hereda una estructura natural de anillo definiendo:

$$\bar{a} + \bar{b} := \overline{a + b}$$
$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}.$$

Es importante señalar que se hace necesario verificar la "buena definición" de estas operaciones. En efecto, la clase $\bar{a}$ no está univocamente determinada por $a$ pues $\bar{a} = \bar{a}_1$ sí y sólo si $a_1 = a + i$, con $i \in I$. Por lo tanto $\bar{a} = \bar{a}_1$ y $\bar{b} = \bar{b}_1$, habrá que verificar que

$$\overline{a + b} = \overline{a_1 + b_1} \qquad \text{y} \qquad \overline{a \cdot b} = \overline{a_1 \cdot b_1}$$

Verifiquemos la segunda. Sean entonces $a_1 = a + i$, $i \in I$, $b_1 = b + i'$, $i' \in I$. Será suficiente probar que $a \cdot b - a_1 \cdot b_1 \in I$. Pero siendo $I$ un ideal esto es una simple verificación:

$$a_1 \cdot b_1 = a \cdot b + i \cdot b + a \cdot i' + i \cdot i'$$

y los tres últimos sumandos pertenecen a $I$ . Que las operaciones así definidas confieren a $A/I$ una estructura de anillo es una verificación inmediata. Obtenemos entonces sobre $A/I$ la estructura de anillo cuociente. La aplicación canónica $f : A \to A/I$ es ahora un morfismo sobre

$$f(a + b) = \overline{a + b} = \bar{a} + \bar{b} = f(a) + f(b)$$

$$f(a \cdot b) = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = f(a) \cdot f(b) .$$

Notar que $f(a) = \bar{a} = 0 \Longrightarrow a \in I$ por lo tanto $Nu(f) = I$ . Hemos pues realizado $I$ como núcleo de un morfismo.

TEOREMA. Sea $P$ un ideal de $A$ . El anillo cuociente $A/P$ es un dominio de integridad sí y sólo si el ideal $P$ es primo.

Demostración: $A/P$ es un dominio de integridad sí y sólo si

$$\overline{x \cdot y} = \bar{x} \cdot \bar{y} = 0 \Rightarrow \bar{x} = 0 \text{ ó } \bar{y} = 0$$

sí y sólo si

$$x \cdot y \in P \Rightarrow x \in P \text{ ó } y \in P$$

lo cual equivale a decir que $P$ es un ideal primo. Veamos ahora un teorema de isomorfismo que es una herramienta básica para trabajar con anillos. Sea $I$ un ideal del anillo $A$ , sea $A'$ un anillo conmutativo y sea $g : A \to A'$ un morfismo. Sea $f : A \to A/I$ el morfismo canónico. Se trata de saber cuándo es posible definir un morfismo $h : A/I \to A'$ tal que $g = h \cdot f$ , o sea tal que el diagrama


sea conmutativo. Se debe verificar entonces que para todo $a \in A$ , $h(f(a)) = g(a)$ .

Como todo elemento de $A/I$ es de la forma $f(a)$ , $a \in A$ , es claro

que si existe $h$ debe cumplirse que $h(f(a)) = g(a)$ . ¿Cuál es el problema entonces? El problema es otra vez, de buena definición. Debe satisfacerse que

$$f(a) = f(b) \Rightarrow g(a) = g(b)$$

o sea $\bar{a} = \bar{b} \Rightarrow g(a) = g(b)$

o sea $a - b \in I \Rightarrow g(a - b) = 0$

o sea $x \in I \Rightarrow g(x) = 0$

o sea, finalmente

$$I \subset Nu(g) .$$

Si pedimos esa condición entonces está garantizada la buena definición de $h$ . Verificar luego que $h$ es morfismo es trivial. Supongamos entonces que se verifique esta condición. Calculemos el núcleo de $h$ . Entonces $h(f(a)) = 0 = g(a)$ , nos dice que

$$Nu(h) = \{f(a) \mid a \in Nu(g)\} ,$$

o sea la imagen de $Nu(g)$ por $f$ . En particular $Nu(h) = 0$ sí y sólo si $Nu(g) = I$ . Finalmente observamos que $h$ es un epimorfismo sí y sólo si $g$ lo es. Reuniendo todos estos resultados se tiene el siguiente resultado fundamental:

TEOREMA. Sea el diagrama de anillos y morfismos


i. Existe un morfismo $h : A/I \to A'$ tal que $h \cdot f = g$ sí y sólo si $I \subset Nu(g)$ .

ii. $Nu(h) = f(Nu(g))$ = imagen por $f$ de $Nu(g)$

iii. $h$ es inyectivo sí y sólo si $Nu(g) = I$ .

iv. $h$ es epimorfismo sí y sólo si $g$ es epimorfismo.

v. $h : A/I \to A'$ es un isomorfismo sí y sólo si $Nu(g) = I$ y $g$ es un epimorfismo.

Este punto v. nos interesa particularmente, pues caracteriza las imágenes de $A$ por morfismos. En efecto, nos dice que si $g : A \to A'$ es un epimorfismo entonces $A'$ es isomorfo al anillo cuociente $A/Nu(g)$. Este es un resultado muy importante. Veamos algunas aplicaciones.

1. Sea $A = \mathbb{R}[X]$, el anillo de polinomios reales. Sea $\mathbb{C}$ el cuerpo complejo. Sea $g : A \to \mathbb{C}$ la aplicación definida por especialización de $X$ por $i$, o sea

$$g\left(\sum_k a_k X^k\right) = \sum_k a_k i^k$$

Esta aplicación es un epimorfismo. Su núcleo lo constituyen todos los polinomios $p(X)$ tales que $p(i) = 0$. Estos constituyen el ideal $\langle X^2 + 1\rangle$ de múltiplos del polinomio $X^2 + 1$. Se sigue del Teorema que $\mathbb{C}$ es isomorfo al anillo cuociente de $\mathbb{R}[X]$ por el ideal $\langle X^2 + 1\rangle$. Así de fácil.

2. Sea $A = \mathbb{Z}[X]$ y sea $I$ el ideal de polinomios con término constante igual a un entero par. Sea $A' = \mathbb{Z}_2$. Sea $g : A \to A'$ definido por composición de morfismos

$$\mathbb{Z}[X] \to \mathbb{Z}_2[X] \to \mathbb{Z}_2$$

$g_1$ reduce los coeficientes de los polinomios módulo 2 y $g_2$ especializa $X$ en 0. El lector puede verificar que el núcleo de $g$ es precisamente $I$. Esto prueba que $I$ es un ideal primo. Como generalización se puede demostrar que los ideales de $\mathbb{Z}[X]$, generados por un primo racional $p$ y un polinomio $p(X)$ que es irreductible módulo $p$ (o sea en $\mathbb{Z}_p[X]$) constituyen ideales primos. Con un poco más de trabajo se puede determinar todos los ideales primos de $\mathbb{Z}[X]$, ejercicio nada despreciable.

Operaciones con ideales.

Sean $I,J$ ideales de un anillo conmutativo $A$. Algunas operaciones importantes con ideales son las siguientes:

i. intersección: $I \cap J$

ii. suma : $I + J := \{i + j \mid i \in I , j \in J\}$

iii. producto : $I \cdot J := \{\Sigma i_r j_r \mid i_r \in I , j_r \in J\}$.

En iii. se toman todas las sumas finitas indicadas. Es una simple verificación que las operaciones definen ideales. En todos los casos las operaciones son asociativas y conmutativas. Para la suma el ideal $0$ es elemento neutro: $I + 0 = I$. Para el producto el ideal $A$ es elemento neutro.

Ejemplo: Sea $A = \mathbb{Z}$ y sean $I = (n)$, $J = (m)$. Entonces $I \cap J = ([n,m])$, $I + J = ((n,m))$, $I \cdot J = (n \cdot m)$. Dos ideales $I,J$ se dicen coprimos si $I + J = A$. Equivalentemente, si existen $i \in I$, $j \in J$ tales que $i + j = 1$.

Una familia finita $I_1, \ldots, I_n$ de ideales se dice coprimos de a dos si $I_r + I_s = A$, si $r \neq s$.

Probamos ahora un resultado clásico fundamental, útil para hallar la solución simultánea de ecuaciones de congruencias. Para el caso de $A = \mathbb{Z}$ este resultado se remonta al período entre el cuarto y el séptimo siglo de nuestra era en que los chinos lo utilizaron para hallar el período común de fenómenos astronómicos.

TEOREMA CHINO DEL RESTO. Sean $I_1, \ldots, I_n$ ideales en $A$ coprimos de a dos. Sean $x_1, \ldots, x_n$ en $A$. Existe $x \in A$ tal que $x \equiv x_i \pmod{I_i}$ para todos los $i$.

Demostración: Si $n = 2$, se tiene

$$1 = i_1 + i_2 \quad , \quad i_r \in I_r \quad , \quad r = 1,2 .$$

Por lo tanto $x = x_2 i_1 + x_1 i_2$ resuelve el problema.

Sean ahora $a_2, \ldots, a_n \in I_1$, $b_2 \in I_2, \ldots, b_n \in I_n$ tales que

$a_i + b_i = 1 \quad , \quad i \geq 2 \ .$

El producto

$$\Pi_{i=2}^{n} (a_i + b_i) = 1$$

está contenido en el ideal

$$I_1 + \Pi_{i=2}^{n} I_i \ .$$

Por lo tanto

$$I_1 + \Pi_{i=2}^{n} I_i = A \ .$$

Utilizando el caso de dos ideales existe $y_1 \in A$ tal que

$$y_1 \equiv 1 (\text{mod } I_1)$$

$$y_1 \equiv 0 (\text{mod } \Pi_{i=2}^{n} I_i) \ .$$

Análogamente utilizando la hipótesis inductiva existen $y_2, \ldots, y_n$ tales que

$$y_2 \equiv 1 (\text{mod } I_2) \quad ; \quad y_2 \equiv 0 (\text{mod } I_j) \quad , \quad j \neq 2 \ ,$$

$$y_3 \equiv 1 (\text{mod } I_3) \quad ; \quad y_3 \equiv 0 (\text{mod } I_j) \quad , \quad j \neq 3 \ ,$$

.....

$$y_n \equiv 1 (\text{mod } I_n) \quad ; \quad y_n \equiv 0 (\text{mod } I_j) \quad , \quad j \neq n \ .$$

El elemento $x = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$ tiene las propiedades pedidas. El teorema queda demostrado.

Para $A = \mathbb{Z}$ se tiene la siguiente formulación. Sean $m_1, \ldots, m_n$ enteros coprimos dos a dos. Sean $x_1, \ldots, x_n$ enteros cualesquiera. Existe entonces un entero $x$ tal que $x \equiv x_i (\text{mod } m_i)$ , para todo $i := 1, \ldots, n$ . Además, en el intervalo entero $[0, \Pi_i m_i)$ hay una única solución.

Aplicación: Sean $I_1, \ldots, I_n$ ideales de $A$ , coprimos de a dos. Sean $A / I_r$ los anillos cuocientes relativos a esos ideales. Formemos el anillo

producto

$$\Pi := A / I_1 \times \ldots \times A / I_n$$

$$= \{(\bar{x}_1, \ldots, \bar{x}_n) \ , \ x_i \in A\}$$

con operaciones componente a componente.

Sea $f : A \to \Pi$ la aplicación definida por

$$f(x) = (x(\text{mod } I_1), x_2(\text{mod } I_2), \ldots, x(\text{mod } I_n)) \ .$$

Es inmediato verificar que $f$ es un morfismo. El Teorema Chino del Resto dice que $f$ es sobre. El núcleo de $f$ es obviamente la intersección de los ideales $I_r$. Según el teorema de isomorfismo se sigue que $A / \cap I_r$ es isomorfo a $\Pi_{r=1}^{n} A / I_r$.

Por ejemplo si $n \in \mathbb{N}$, $n = p_1^{e_1} \ldots p_r^{e_r}$, con $p_i$ primos distintos, se tiene el isomorfismo (de anillos):

$$\mathbb{Z}_n \approx \mathbb{Z}_{p_1^{e_1}} \times \ldots \times \mathbb{Z}_{p_r^{e_r}} \ .$$

Ejercicios:

1. Caracterizar los anillos cuocientes: $\mathbb{Z}[i] / (3)$, $\mathbb{Z}[i] / (5)$, $\mathbb{Z}[i] / (3 + 2i)$, $\mathbb{Z}[i] / (2i)$, $\mathbb{Z}[i] / (1 + i)$.

2. Sea $q \in \mathbb{N}$, primo de la forma $4m + 3$. Caracterizar $\mathbb{Z}[i] / (q)$.

3. Sea $q \in \mathbb{N}$ primo de la forma $4m + 3$. Sea $z = a + bi \in \mathbb{Z}[i]$. Probar que $z^q \equiv \bar{z} (\text{mod } q)$.

9. Ideales en $\mathbb{Z}[\sqrt{-5}]$

Sea $I$ un ideal de $A = \mathbb{Z}[\sqrt{-5}]$, $I \neq 0$. Si $x \in I$, $x \neq 0$ entonces $N(x) \neq 0$ es un entero en $I$, por lo tanto $I \cap \mathbb{Z} = (a)$, $a \neq 0$ es un ideal en $\mathbb{Z}$. Se sigue que si $m \in I \cap \mathbb{Z}$ entonces $a \mid m$. Se tiene entonces la inclusión $(a) \subset I$.

Sea ahora $b$ máximo divisor común de todos los $y \in \mathbb{Z}$ con la propiedad que existe $x \in \mathbb{Z}$ con la propiedad $x + y\sqrt{-5} \in I$. Notar que la totalidad de tales enteros $y$, es un ideal en $\mathbb{Z}$, por lo tanto el mismo es generado por un elemento $b$, que tomaremos además positivo. Se sigue entonces que

$$x + y\sqrt{-5} \in I \Leftrightarrow b \mid y .$$

Además, dado que $a \in I$, $a\sqrt{-5} \in I$ y por lo tanto $b \mid a$.
Sea $x + b\sqrt{-5} \in I$. Si $x = a \cdot q + r$, $0 \leq r < a$ entonces

$$x + b\sqrt{-5} = x - a \cdot q + b\sqrt{-5} = a \cdot q + x + b\sqrt{-5} \in I$$

Además $r + b\sqrt{-5} \in I \Leftrightarrow -5b + r\sqrt{-5} \Leftrightarrow b \mid r$.

Por lo tanto hemos determinado enteros $b, a, r$, no negativos con las propiedades $b \mid a$, $b \mid r$.

Afirmación: Todo elemento de $I$ se escribe en forma unívoca en la forma

$$ma + n(r + b\sqrt{-5}), \qquad m,n \in \mathbb{Z}.$$

Demostración: Es claro que $\forall\, m,n \in \mathbb{Z}$, $ma + n(r + b\sqrt{-5}) \in I$. Sea recíprocamente, $u + v\sqrt{-5} \in I$. Sea $v = b \cdot n$, $n \in \mathbb{Z}$, se tiene

$$u + v\sqrt{-5} = u - nv + n(r + b\sqrt{-5})$$

y por lo tanto $u - nv \in I \cap \mathbb{Z}$, o sea $u - nv = ma$ y podemos escribir

$$u + v\sqrt{-5} = ma + n(r + b\sqrt{-5}) .$$

Además $ma + n(r + b\sqrt{-5}) = m'a + n'(r + b\sqrt{-5})$, $m,m',n,n'$ en $\mathbb{Z}$ implican $(m - m')a = (n' - n)(r + b\sqrt{-5})$

o sea $(n' - n)b = 0$, o también $n = n'$ y $m = m'$.

Hemos probado entonces que el ideal $I$ posee un sistema de generadores formados por dos elementos $a \in \mathbb{Z}$ y $r + b\sqrt{-5}$. O sea

$$I = (a,r + b\sqrt{-5}) .$$

Los elementos $a,r + b\sqrt{-5}$ los llamaremos <u>generadores canónicos de</u> $I$ o también que $(a,r + b\sqrt{-5})$ es la expresión canónica del ideal $I$ .

<u>Observación:</u> El ideal es generado por $a$ y $r + b\sqrt{-5}$ <u>sobre</u> $\mathbb{Z}$ , es decir utilizando combinaciones <u>enteras</u> de $a$ y $r + b\sqrt{-5}$ . Hay por lo tanto un abuso de notación. Por ejemplo el ideal $I = (1 + \sqrt{-5})$ , es un ideal principal generado por $1 + \sqrt{-5}$ . Consta de todos los múltiplos de $(1 + \sqrt{-5})$ en $\mathbb{Z}[\sqrt{-5}]$ . Su forma canónica es $(6,1 + \sqrt{-5})$.

Caractericemos los ideales primos de $\mathbb{Z}[\sqrt{-5}]$ . Sea $P = (a,r + b\sqrt{-5})$ un ideal primo en $\mathbb{Z}[\sqrt{-5}]$ , $P \neq 0$ . Entonces $P \cap \mathbb{Z} = (p)$ , $p$ primo $> 0$ , pues $\mathbb{Z} \cap P$ es un ideal primo en $\mathbb{Z}$ . Además

$$N(r + b\sqrt{-5}) = r^2 + 5b^2 \equiv 0 (\text{mod } p)$$

por ser un elemento de $P \cap \mathbb{Z}$ .

Puesto que $b \mid p$ , hay dos posibilidades $b = 1$ ó $b = p$ .

Si $b = p$ entonces $P = (p)$ , pues $b \mid r$ .

Si $b = 1$ entonces $r^2 + 5 \equiv 0 (\text{mod } p)$ y $-5$ es residuo cuadrático módulo $p$ , o sea, utilizando el símbolo de Legendre $\left(\frac{-5}{p}\right) = 1$ . Recíprocamente supongamos $r$ satisface $r^2 + 5 \equiv 0 (\text{mod } p)$ . Afirmamos que $(p,r + \sqrt{-5})$ es ideal primo en $\mathbb{Z}[\sqrt{-5}]$ .

A este fin sea $f : [\sqrt{-5}] \to \mathbb{Z}_p$ el morfismo definido por

$$f(x + y\sqrt{-5}) = \bar{x} - \bar{y}\cdot\bar{r}$$

donde la barra superior denota la clase módulo $p$ . Notar que la condición $r^2 \equiv -5 (\text{mod } p)$ indica que $\bar{r}^2 = -5$ en $\mathbb{Z}_p$ . Es claro que $P \subset Nu(f)$ . Veamos que $P = Nu(f)$ . Sea $f(x + y\sqrt{-5}) = \bar{x} - \bar{y}\cdot\bar{r} = 0$ .

Se sigue que $x = yr + pt$ , por lo tanto $x + y\sqrt{-5} = pt + y(r + \sqrt{-5}) \in P$ .

Concluimos que $P$ es un ideal primo. Además

$$\mathbb{Z}[\sqrt{-5}] / (p,r + \sqrt{-5}) \approx \mathbb{Z}_p .$$

Sea p primo impar positivo tal que $\left(\frac{-5}{p}\right) = -1$ . Afirmamos que el ideal principal $P = (p)$ es primo. Repitiendo el razonamiento anterior, sea $\mathbb{Z}(u)$ el anillo formado por los pares $x + y\cdot u$ , con $x,y$ en $\mathbb{Z}_p$ y $u$ un símbolo con la propiedad $u^2 = -5$ (esta construcción imita los números complejos, pero sobre el cuerpo $\mathbb{Z}_p$). El hecho que en $\mathbb{Z}_p$ la ecuación $x^2 + 5 = 0$ no admite solución implica que $\mathbb{Z}_p(u)$ es un cuerpo. Si definimos el morfismo $f : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_p(u)$ por

$$f(x + y\sqrt{-5}) = \bar{x} + \bar{y}\cdot u$$

verificamos fácilmente que $Nu(f) = P$ , lo cual demuestra que $P = (p)$ es un ideal primo.

Se tiene entonces que los ideales primos de $\mathbb{Z}[\sqrt{-5}]$ son:

i. $(p)$ , $p$ primo $> 0$ , $p \neq 2,5$ con $\left(\frac{-5}{p}\right) = -1$ .

ii. $p$ primo $> 0$ , $(p, r + \sqrt{-5})$ , con $r^2 \equiv -5 (\text{mod } p)$ .

En ii. figuran los ideales $(2, 1 + \sqrt{-5})$ y $(\sqrt{-5})$ .

Un Corolario de esta clasificación es que todo ideal primo de $\mathbb{Z}[\sqrt{-5}]$ es maximal. En efecto, un ideal $P$ de un anillo conmutativo $A$ es maximal sí y sólo si el anillo cuociente $A/P$ es un cuerpo.

Ejemplos:

i. Sea $p = 3$. Dado que $r^2 \equiv -5 (\text{mod } 3)$ admite soluciones $r = 1$ y $r = 2$ . Por lo tanto se tienen los ideales $P = (3, 1 + \sqrt{-5})$ , $P' = (3, 2 + \sqrt{-5})$ .

Estos ideales son distintos. En efecto, $P = P'$ implica que $1 = 2 + \sqrt{-5} - (1 + \sqrt{-5}) \in P$ .

Calculemos el producto $P\cdot P'$

$$P\cdot P' = (3, 1 + \sqrt{-5}) \cdot (3, 2 + \sqrt{-5}) =$$

$$= (9, 6 + 3\sqrt{-5}, 3 + 3\sqrt{-5}, -3 + 3\sqrt{-5})$$

$$= (9, 6 + 3\sqrt{-5}, 3, -3 + 3\sqrt{-5}) = (3) .$$

Esto nos dice que el ideal principal 3 se factoriza en producto de

ideales primos $(3) = P \cdot P'$ .

ii. $p = 7$ . Dado que $r^2 \equiv -5 (\text{mod } 7)$ admite soluciones $r = 4$ , $r = 3$ . Por lo tanto se tienen los ideales $Q = (7, 4 + \sqrt{-5})$ , $Q' = (7, 3 + \sqrt{-5})$ , y satisfacen $(7) = Q \cdot Q'$ .

Con $P, P'$ , $Q, Q'$ obtenemos la factorización del ideal principal $(21)$ en producto de ideales primos $(21) = P \cdot P' \cdot Q \cdot Q'$ y esto nos servirá para recomponer la factorización única, pero en producto de ideales primos. En efecto

$$P \cdot Q' = (3, 1 + \sqrt{-5}) \cdot (7, 3 + \sqrt{-5}) =$$

$$= (21, 9 + 3\sqrt{-5}, 7 + 7\sqrt{-5}, -2 + 4\sqrt{-5})$$

$$= (21, -11 + \sqrt{-5}, 7 + 7\sqrt{-5}) = (21, -22 + 2\sqrt{-5}, 7 + 7\sqrt{-5})$$

$$= (-1 + 2\sqrt{-5})$$

$$= (1 - 2\sqrt{-5}) .$$

Análogamente

$$P' \cdot Q = (1 + 2\sqrt{-5})$$

$$P \cdot Q = (4 + \sqrt{-5})$$

$$P' \cdot Q' = (4 - \sqrt{-5})$$

Por lo tanto la factorización

$$(21) = P \cdot P' \cdot Q \cdot Q'$$

$$(3) \cdot (7) = (P \cdot P')(Q \cdot Q')$$

$$((1 + 2\sqrt{-5})) \cdot ((1 - 2\sqrt{-5})) = (P' \cdot Q)(P \cdot Q')$$

$$((4 + \sqrt{-5})) \cdot ((4 - \sqrt{-5})) = (P \cdot Q)(P' \cdot Q') .$$

El ideal primo $P = (2, 1 + \sqrt{-5})$ satisface $P^2 = (2)$ . Igualmente el ideal $(\sqrt{-5})$ es primo y satisface $(\sqrt{-5})^2 = (5)$ .

TEOREMA. Sea $I = (a, r + b\sqrt{-5})$ y sea $I' = (a, r - b\sqrt{-5})$ . Entonces $I \cdot I' = (d)$ , con $d \in N \cup 0$ .

Demostración: Escribamos $a = ba'$ , $r = br'$ . Entonces

$$I \cdot I' = (b^2)(a', r' + \sqrt{-5})(a', r' - \sqrt{-5})$$

$$= (b^2)(a'^2, a'r' - a'\sqrt{-5}, a'r' + a'\sqrt{-5}, r'^2 + 5) .$$

Puesto que $(a', r' + \sqrt{-5}) \cdot (a', r' - \sqrt{-5}) \subset (a', r' + \sqrt{-5})$ se sigue que $r'^2 + 5$ es divisible por $a'$ y entonces lo anterior es igual a

$$= (b^2)(a')\left(a', r' - \sqrt{-5}, r' + \sqrt{-5}, \frac{r'^2 + 5}{a'}\right)$$

Probemos que el ideal $J = \left(a', r' - \sqrt{-5}, r' + \sqrt{-5}, \frac{r'^2 + 5}{a'}\right) = (1) = \mathbb{Z}[\sqrt{-5}]$ .

Notemos que $2\sqrt{-5} \in J$ y por lo tanto $10 \in J$ . Por lo tanto $J$ contiene al máximo común divisor $(a', 10)$ . Los valores posibles de este mcd son $1, 2, 5, 10$ . Si es 1 nada hay que probar. Sea entonces $2 \in J$ . Entonces $r'^2 + 5 = a' \cdot 2 \cdot h = 4h'$ , pues $2 \mid a'$ .
Se sigue que $r'$ es impar. Por lo tanto módulo 4 resulta $1 + 1 \equiv 0 (\text{mod } 4)$ una contradicción. Sea $5 \in J$ , se tiene $r'^2 + 5 = 5 \cdot a' \cdot t = 5^2 \cdot h'$ pues $5 \mid a'$ .
Pero $2r' \in J$ , y es así divisible por 5. Entonces $5^2$ divide a $r'^2$ . Lo anterior dice que $5^2 \mid 5$ , un absurdo.
Sea $10 \in J$ . Otra vez escribimos $r'^2 + 2 = 10^2 \cdot h$ , de donde se sigue que $r'$ es impar. Módulo 4 nos dá una contradicción. Concluimos que $1 \in J$ y hemos probado que

$$I \cdot I' = (b^2 a') = (ab) .$$

COROLARIO FUNDAMENTAL. Sean $I \subset J$ ideales, $J \neq 0$ . Existe un ideal $B$ tal que $I = J \cdot B$ .

Demostración: Sea $d \in \mathbb{Z}$ , $d \neq 0$ , tal que $J \cdot J' = (d)$ . Por lo tanto $I \cdot J' \subset (d)$ .
Notemos que para cualquier anillo $A$ , y $d \in A$ , la aplicación $A \to dA$ , multiplicación por $d$ , aplica biyectivamente los ideales de

$A$ en ideales de $A$ contenidos en $dA$. Por lo tanto $I \cdot J' = (d) \cdot B$ con $B$ ideal en $\mathbb{Z}[\sqrt{-5}]$. Por lo tanto

$$(d) \cdot I = I \cdot J \cdot J' = (d) \cdot B \cdot J$$

pero $\mathbb{Z}[\sqrt{-5}]$ es un dominio de integridad (multiplicar por $d \neq 0$ es una aplicación inyectiva). Concluimos que $I = J \cdot B$.

DEFINICION. Sean $I,J$ ideales. Decimos que $I$ divide a $J$, $I \mid J$, si existe un ideal $B$ tal que $J = I \cdot B$.

El Corolario dice exactamente que: $I \subset J \Longrightarrow J \mid I$.

COROLARIO. Sea $P$ un ideal primo y sean $I,J$ ideales. Entonces

$$P \mid I \cdot J \Longrightarrow P \mid I \text{ ó } P \mid J .$$

Demostración: $P \mid I \cdot J \Longrightarrow I \cdot J \subset P \Longrightarrow I \subset P$ ó $J \subset P \Longrightarrow P \mid I$ ó $P \mid J$.

TEOREMA. Todo ideal $I \neq 0$ es producto de ideales primos en forma unívoca.

Demostración: Si $I$ es un ideal maximal de $\mathbb{Z}[\sqrt{-5}]$ entonces $I$ es primo y nada hay que probar. Sea $P_1$ un ideal maximal (luego primo) que contiene a $I$.

NOTA. Ya probamos que todo ideal primo es maximal. Además todo ideal $I \neq 0$ está contenido en un ideal maximal dado que el anillo cuociente $\mathbb{Z}[\sqrt{-5}] / I$ es un anillo finito. Dejamos a cargo del lector probar esta afirmación.

Sea entonces $P_1$ un ideal primo tal que $I \subset P_1$. Entonces existe un ideal $I_1$ tal que $I = P_1 \cdot I_1$. Podemos repetir el razonamiento con $I_1$ y obtener una factorización $I = P_1 \ldots P_k \cdot I_k$ con $P_i$ ideales primos. Se trata de ver que el proceso no puede seguir indefinidamente. Para ello formemos el ideal $I' = P_1' \ldots P_k' \cdot I_k'$, con $I \cdot I' = (a)$, $P_i \cdot P_i' = (p_i)$, $I_k \cdot I_k' = (d)$. Multiplicando obtenemos

$(a) = (p_1)\cdot(p_2) \ldots (p_k)\cdot(d_k)$ en $Z$.

Dado que $a$ posee sólo un número finito de divisores queda probado que el proceso de factorización de $I$ en producto de ideales primos es finito y esto prueba que todo ideal $\neq 0$ es producto de ideales primos. Veamos la unicidad. Sean $P_1\cdot P_2 \ldots P_k = Q_1\cdot Q_2 \ldots Q_r$, con $P_i, Q_j$ ideales primos. Entonces $P_1 \supset Q_1\cdot Q_2 \ldots Q_r$ y debe verificarse que $Q_i \subset P_1$ para algún ideal primo $Q_i$. Dado que todo ideal primo $\neq 0$ es maximal concluimos que $P_1 = Q_i$. Multiplicando por $P_1^{-1}$ y cancelando resulta

$$P_2 \ldots P_k = Q_1 \ldots \hat{Q}_i \ldots Q_r$$

donde $\hat{\ }$ indica que hay que omitir el índice. Razonando ahora inductivamente concluimos que $k - 1 = r - 1$, o sea $k = r$ y salvo permutación los ideales $P_i, Q_i$ son los mismos.

Hemos demostrado entonces la validez de un Teorema Fundamental de la Aritmética para Ideales. Puesto que los elementos de $\mathbb{Z}[\sqrt{-5}]$ se pueden identificar a ideales principales, esta teoría generaliza la divisibilidad ordinaria, pero tiene de bueno que agrega la factorización única.

10. APENDICE.

Vamos a analizar más cuidadosamente la introducción de factores ideales en $\mathbb{Z}[\sqrt{-5}]$ , disponiendo ahora del material precedente:

Vamos a caracterizar el anillo cuociente $\mathbb{Z}[\sqrt{-5}]/(3)$ de $\mathbb{Z}[\sqrt{-5}]$ por el ideal generado por el elemento 3. Para ello buscamos una imagen homomorfica de $\mathbb{Z}[\sqrt{5}]$ conveniente. Sea $A$ el anillo de pares ordenados $(x,y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ , dotado de suma y producto como en los números complejos ordinarios pero con la variante siguiente: Escribimos $(x + \alpha y)$ en lugar de $(x,y)$ y se satisfacen:

$$x + \alpha y = x' + \alpha y' \qquad x = x' \ , \quad y = y'$$

$$(x + \alpha y) + (x' + \alpha y') = (x + x' + \alpha(y + y'))$$

$$(x + \alpha y)(x' + \alpha y') = (xx' + yy' + \alpha(x'y + xy')$$

Notar que $\alpha^2 = 1$ .

Entonces la aplicación

$$\mathbb{Z}[\sqrt{-5}] \xrightarrow{\ \phi\ } A$$

$$x + y\sqrt{-5} \longmapsto x - \alpha y$$

es un epimorfismo cuyo núcleo es precisamente el ideal $(3)$ . Dejamos los detalles de verificación a cargo del lector. Llamando $e_1 = 2 + \alpha$ , $e_2 = 2 - \alpha$ en $A$ , resulta que $e_1^2 = e_1$ , $e_2^2 = e_2$ , $e_1 e_2 = 0$ , $e_1 + e_2 = 1$ . Esto dá una descomposición de $A$ en suma directa $\mathbb{Z}_3 e_1 \oplus \mathbb{Z}_3 e_2$ de cuerpos isomorfos a $\mathbb{Z}_3$ .

Calculemos $\phi^{-1}(\mathbb{Z}_3 e_i) = S_i$ , $\quad i = 1,2, \ldots$

Entonces si $z = x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ ,

$$\phi(z) = \overline{x} + \alpha\overline{y} \in \mathbb{Z}_3 e_1$$

— es anulado por $e_2$ , o sea

$$0 = (\overline{x} + \alpha\overline{y})(2 - \alpha) = 2\overline{x} + 2\alpha\overline{y} - \alpha\overline{x} - \overline{y}$$

$$= (2\overline{x} - \overline{y}) - \alpha(-\overline{y} + 2\overline{x})$$

o sea $2x \equiv y \pmod 3$ .

Entonces $J_1 = \{x + y\sqrt{-5} \mid 2x \equiv y(3)\}$

$$= \{x + y\sqrt{-5} \mid x \equiv -y(3)\}$$

$$= \{y(-1 + \sqrt{-5}) + 3t \mid y,t \in \mathbb{Z}\}$$

$$= 3\mathbb{Z} + (-1 + \sqrt{-5})\mathbb{Z}$$

y análogamente

$$J_2 = 3\mathbb{Z} + (1 + \sqrt{-5})\mathbb{Z} .$$

Una verificación nos muestra que

$$J_1 J_2 = (3)$$

y esto dá otra introducción de factores ideales. En este caso se trata concretamente de ideales.

El anillo $\mathbb{Z}[\rho]$ de enteros de Eisenstein.

Se trata del anillo obtenido adjuntando a $\mathbb{Z}$ una raíz cúbica primitiva $\rho$ de la unidad. O sea $\rho$ satisface

$$\rho^2 + \rho + 1 = 0 .$$

Los elementos de $\mathbb{Z}[\rho]$ son de la forma $a + b\rho$ con $a,b \in \mathbb{Z}$ .

Este anillo no es otra cosa que el anillo de enteros de la extensión cuadrática $Q(\sqrt{-3})$ . Dado que $-3 \equiv 1 \pmod 4$ los enteros de $Q(\sqrt{-3})$ son los números de la forma

$$a + b\,\frac{1 + \sqrt{-3}}{2} , \qquad a,b \in \mathbb{Z}$$

o también

$$\frac{a + b\sqrt{-3}}{2} \quad \text{con} \quad a,b \in \mathbb{Z} \ , \quad a \equiv b (\text{mod } 2) \ .$$

Dado que $\rho = \frac{-1 + \sqrt{-3}}{2}$ y $\rho^2 = \frac{-1 - \sqrt{-3}}{2}$ están en $\mathbb{Z}[\rho]$ es claro que estos anillos coinciden.

Sea $z = a + b\rho \in \mathbb{Z}[\rho]$ . El conjugado de $z$ es $\overline{z} = a + b\overline{\rho}$ . Se define la norma de $z$ por

$$N(z) = z\overline{z} = a^2 - ab + b^2$$

y se verifican las propiedades de las normas

$$N(z_1 \cdot z_2) = N(z_1)N(z_2)$$

$$N(1) = 1 \ .$$

Puesto que $a^2 - ab + b^2 = (a - b)^2 + ab$ se sigue que $N(z) \geq 0$ y es $= 0 \iff z = 0$ .

Las unidades de $\mathbb{Z}[\rho]$ están caracterizadas por la propiedad $N(z) = 1$ .

Dejamos a cargo del lector verificar que hay en total 6 unidades, a saber

$$\pm 1 \ , \ \pm\rho \ , \ \pm\rho^2 \ .$$

Podemos ver que $\mathbb{Z}[\rho]$ es un dominio euclídeo vía la norma, como ocurre en $\mathbb{Z}[i]$ . Para ello basta probar que todo $t = r + s\rho \ ; \ r,s \in \mathbb{Q}$ se puede aproximar, en norma, en menos de 1 .

Si $a,b \in \mathbb{Z}$ son tales que $|r - a| \leq \frac{1}{2}$ , $|s - b| \leq \frac{1}{2}$ entonces

$$N(t - (a + b\rho)) = (r - a)^2 - (r - a)(s - b) + (s - b)^2$$

$$\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4} < 1 \ .$$

De esta manera vale un lema de aproximación y con ello la existencia de algoritmo de división. Concretamente $\mathbb{Z}[\rho]$ es un dominio de factorización única.

Hallemos los primos de Eisenstein.

Sea $\pi \in \mathbb{Z}[\rho]$ tal que $N(\pi) = p$ es un primo racional. Entonces está claro que $\pi$ es un primo en $\mathbb{Z}[\rho]$ (por la multiplicidad de la norma).

Sea ahora $\pi \in \mathbb{Z}[\rho]$ primo. Supongamos $N(\pi)$ no es primo racional, entonces $N(\pi) = a \cdot b$, $a > 1$, $b > 1$ en $\mathbb{Z}$. O sea $\pi\bar{\pi} = a \cdot b$. Entonces $\pi \mid a$ ó $\pi \mid b$. Supongamos $\pi \mid a$. Se tiene $\bar{\pi} = \frac{a}{\pi} b$ en $\mathbb{Z}[\rho]$. Como $\bar{\pi}$ es primo, $\frac{a}{\pi} = u$ ó $b$ asociado a $\bar{\pi}$.

En cualquier caso se sigue que

$$a = b \quad \text{o sea} \quad N(\pi) = a^2$$

y $\quad a \sim \pi \quad$ o sea $a$ es primo racional (y primo en $\mathbb{Z}[\rho]$).

Por lo tanto: $\pi \in \mathbb{Z}[\rho]$ es primo sí y sólo si

i) $N(\pi) = p$ un primo racional, o

ii) $N(\pi) = p^2$, $p$ primo racional y $\pi$ es asociado a un primo racional que es primo en $\mathbb{Z}[\rho]$.

EJEMPLOS: i) Sea $\lambda = 1 - \rho$. Entonces

$$N(\lambda) = (1 - \rho)(1 - \bar{\rho}) = (1 - \rho)(1 - \rho^2) = 1 - \rho^2 - \rho + 1 = 3$$

por lo tanto $\lambda$ es primo en $\mathbb{Z}[\rho]$.

ii) $7 = (2 + \sqrt{-3})(2 - \sqrt{-3})$ con $N(2 + \sqrt{-3}) = N(2 - \sqrt{-3}) = 7$ por lo tanto 7 no es primo en $\mathbb{Z}[\rho]$.

iii) 11 es primo en $\mathbb{Z}[\rho]$. En efecto, $11 = z \cdot v$ implica que $11 = N(z)$ y escribiendo $z = \frac{a + b\sqrt{-3}}{2}$ resulta:

$$a^2 + 3b^2 \equiv 0 \pmod{11}$$

o sea $\quad \left(\frac{-3}{11}\right) = 1$. Pero $\left(\frac{-3}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{3}{11}\right) =$

$$(-1)(-1)\left(\frac{11}{3}\right) = \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

una contradicción.

Notar que el razonamiento vale para todo primo $p$ tal que $p \equiv 2 \pmod 3$.

En particular 2 es primo en $\mathbb{Z}[\rho]$ .

iv) Si $p \equiv 1(3)$ , entonces $\left(\frac{-3}{p}\right) = 1$ . En efecto,

a) si $p = 4m + 3$ , $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = -1 \cdot 1\left(\frac{p}{3}\right) = 1$

b) si $p = 4m + 1$ , $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right) = 1$

por lo tanto si $r \in \mathbb{Z}$ satisface $r^2 + 3 \equiv 0(p)$ se tiene

$$(r + \sqrt{-3})(r - \sqrt{-3}) = p \cdot \alpha$$

Si $p$ fuera primo en $\mathbb{Z}[\rho]$ entonces

$$p \mid r + \sqrt{-3} \qquad y \qquad p \mid r - \sqrt{-3}$$

o sea $p \mid 3$ , imposible pues $p \equiv 1(3)$ .

Por lo tanto $p = z_1 \cdot z_2$ o sea $p^2 = N(z_1) \cdot N(z_2)$ o sea $N(z_1) = p$ y $N(z_2) = p$ . O sea $p = z_1 \bar{z}_1 = z_2 \bar{z}_2$ , con $z_1$ asociado a $z_2$ ó a $\bar{z}_2$ . En definitiva $p = z \cdot \bar{z}$ , con $z$ primo en $\mathbb{Z}[\rho]$ .

v) Notemos la factorización de 3.

$$3 = N(1 - \rho) = (1 - \rho)(1 - \bar{\rho}) = (1 - \rho)(1 - \rho^2) =$$

$$= (1 - \rho)(\rho^3 - \rho^2) = \rho^2(1 - \rho)(\rho - 1) = -\rho^2\lambda^2$$

Determinemos ahora algunos anillos cuocientes de $\mathbb{Z}[\rho]$ por ideales primos

i) $\mathbb{Z}[\rho] / _{(\lambda)}$ , donde $\lambda = 1 - \rho$ . Si $z = a + b\rho \in \mathbb{Z}[\rho]$ escribimos $z = a + b\rho = a + b - \lambda b$ y si $a + b = 3 \cdot k + r$ , con $r = 0, 1, -1$ , resulta

$$z = r + \lambda \cdot t \qquad \text{con } N(r) < N(\lambda) = 3$$

Por lo tanto $\mathbb{Z}[\rho] / _{(\lambda)} \simeq \mathbb{Z}_3$ .

ii) Sean los primos de norma 7, $2 + \sqrt{-3}$ y $2 - \sqrt{-3}$ .

Se tiene $7 = (2 + \sqrt{-3})\cdot(2 - \sqrt{-3})$ .

Como $7 \equiv 1(3)$ , en el grupo $\mathbb{Z}_7^*$ hay una raíz cúbica primitiva de la unidad, a saber 2 y por supuesto también 4. Ambas son raíces de la ecuación en $\mathbb{Z}_3$:

$$x^2 + x + 1 = 0$$

Por lo tanto hay dos morfismos $\mathbb{Z}[\rho] \to \mathbb{Z}_7$ dados por

$$a + b\rho \xmapsto{\phi_1} a + 2b$$

y $$a + b\rho \xmapsto{\phi_2} a + 4b .$$

En ambos casos se tienen epimorfismos.

Calculemos los núcleos. Hagamoslo para $\phi_1$ . Es claro que $\phi_1(2 + 2\rho) = 0$ . Recíprocamente si $\phi_1(a + b\rho) = 0$ entonces $a + 2b \equiv 0(\text{mod } 7)$ , o sea $b \equiv -4a(\text{mod } 7)$ .

Por lo tanto

$$a + b\phi \equiv a + 6a - 2a(2 + 2\rho)(\text{mod } 7)$$

o sea $$a + b\phi \equiv -2a(3 + 2\rho)(\text{mod } 7)$$

de lo cual se sigue que $a + b\phi$ pertenece al ideal generado por $3 + 2\rho$ , con lo que concluimos que $Nu(\phi_1) = (3 + 2\rho)$ .

Análogamente $Nu(\phi_2) = (3 - 2\rho)$ .

Notar que $7 = (3 + 2\rho)(3 - 2\rho)$ . Se puede ver que

$$(3 + 2\rho) \cap (3 - 2\rho) = (7) .$$

iii) Sea $\pi$ un primo cuya norma $N(\pi) = p^2$ . Entonces $p \equiv 2(\text{mod } 3)$ , lo cual implica que en $\mathbb{Z}_p^*$ no hay raíces cúbicas primitivas de la unidad. Imitando los complejos extendemos $\mathbb{Z}_p$ al anillo de pares ordenados $a + b\alpha$ , $a,b \in \mathbb{Z}_p$ con las operaciones ordinarias de los complejos pero

con la relación

$$\alpha^2 + \alpha + 1 = 0 .$$

Es claro que obtenemos un cuerpo que denotaremos por $K$ . Definimos ahora

$$\mathbb{Z}[\rho] \xrightarrow{\phi} K$$

por $\qquad a + b\rho \to a + b\alpha .$

Dado que $\pi$ es asociado con $p$ , $\phi(\pi) = 0$ . Ahora $\phi(a + b\rho) = \bar{a} + \bar{b}\alpha = 0$ implica

$$a \equiv b \equiv 0 (\mathrm{mod}\ p)$$

por lo tanto $a + b\rho$ es múltiplo de $\pi$ y esto muestra que $Nu(\phi) = (\pi)$ . En este caso $\mathbb{Z}[\rho]/(\pi)$ tiene $p^2$ elementos.

El ejemplo considerado en ii) se extiende a todos los primos $p \equiv 1 (\mathrm{mod}\ 3)$ , de manera que hemos cubierto en general la determinación de los cuocientes de $\mathbb{Z}[\rho]$ por ideales primos.

El anillo de enteros de $Q(\sqrt{-2})$

Se trata del anillo $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a,b \in \mathbb{Z}\}$ .

Dejamos como ejercicio probar que

1. $\mathbb{Z}[\sqrt{-2}]$ es un dominio euclídeo y por lo tanto un DFU.

2. Los primos de $\mathbb{Z}[\sqrt{-2}]$ son de la siguiente forma:

   i. los números $\pm p$ , con $p$ primo racional, $p \equiv 5$ ó $p \equiv 7 (\mathrm{mod}\ 8)$ respectivamente.

   ii. los enteros $x + y\sqrt{-2}$ cuyas normas son primos racionales $p \equiv 1$ ó $p \equiv 3 (\mathrm{mod}\ 8)$ respectivamente

   iii. $\sqrt{-2}$ .

   [Sugerencia: Usar las leyes de reciprocidad cuadrática suplementarias

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} , \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} , \quad p \text{ primo impar}]$$

3. Hallar todas las soluciones enteras de la ecuación $y^2 + 2 = x^3$ .

BIBLIOGRAFIA.

1. Textos Elementales.

GENTILE E.R., Aritmética Elemental, Monografía N° 25 de la serie Matemática (Textos azules) de la OEA (1985).

GENTILE, E.R., Notas de Algebra, EUDEBA (1988).

NIVEN, I. y ZUCKERMAN, H., An introduction to the theory of Numbers, Wiley, New York, N.Y. (1972).

SHOCKELEY, J.E.., Introduction to Number Theory, Holt, Rinehart & Winston, Inc. New York, N.Y. (1967).

STARK, H., An introduction to Number Theory, Markham, Chicago, III (1970).

USPENSKY, J. y HEASLET, M.A., Elementary Number Theory, McGraw, New York, N.Y. (1939).

VINOGRADOV, I., Fundamentos de la Teoría de Números, Editorial Mir, Moscú (1971).

2. Textos más Avanzados.

HARDY, G.H. y WRIGHT, E.M., An introduction to the Theory of Numbers, Oxford Univ. Press, Londres, 4a. edición (1962).

HASSE, H., Vorlesungen über Zahlentheorie, Springer-Verlag, Berlín (1964).

3. Referencias de tipo histórico.

DICKSON, L., History of the Theory of Numbers, Chelsea Publishing Co., Nueva York, N.Y., 3 vols. (1952).

ORE, O., Number Theory and its history, McGraw, Nueva York, N.Y. (1948).

4. Textos sobre la Teoría Algebraica de Números.

BOREVICH, Z.I. y SHAFAREVICH, I.R., Number Theory, Academic, Londres (1966).

DIAMOND, H. y POLLARD, H., The Theory of algebraic numbers, Mathematical Association of America, Carus Mathematical Monographs, Washington, D.C. (1985).

IRELAND, K. y ROSEN, M., A classical introduction to modern Number Theory, Springer-Verlag, Berlín (1982).

5. Misceláneos.

DAVENPORT, H., The higher Arithmetic, Harper, Nueva York, N.Y. (1960).

KRAITCHIK, M., Mathematical recreations, Dover, Nueva York, N.Y. (1960).

KNUTH, D.E., The art of computer programming, Addison-Wesley, Reading, Mass., vol. 2 (1969).

SIERPINSKI, M., A selection of problems in the Theory of Numbers, MacMillan, Nueva York, N.Y. (1964).

The William Lowell Putnam Mathematical Competition. Problems and Solutions, 1938-1964, Mathematical Association of America, Washington, D.C. (1980).

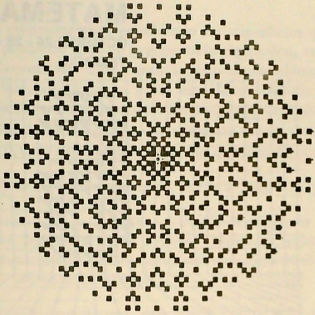
6. Revistas.

Un gran número de artículos sobre la Teoría de Números, así como también sobre problemas propuestos, aparecen en las siguientes revistas publicadas por la Mathematical Association of America: Year College, Journal of Mathematics, Mathematics Magazine y American Mathematical Montly. Una excelente revista que presenta artículos de divulgación en Scientific American.

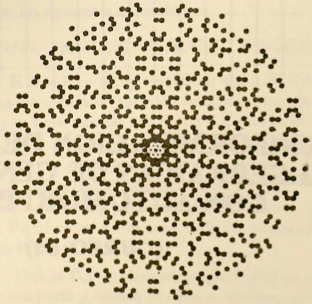
Departamento de Matemáticas
Facultad de Ciencias
Universidad de Chile
Casilla 653.Santiago
CHILE.

Departamento de Matemáticas
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria. Pabellón I
1428 Núñez
Buenos Aires
ARGENTINA.

DIAGRAMAS TOMADOS DE R. GUY : Unsolved Problems in Number Theory (Springer).



Primos de Gauss de norma menor que 1000.



Primos de Eisenstein