ESTRUCTURAS ALGEBRAICAS. GRUPO M3 (19-20).
CARLOS ANDRADAS Y ANDONI DE ARRIBA.

Divisibilidad en anillos. Elementos primos e irreducibles.

1. Dado $n \in \mathbb{Z}$ libre de cuadrados[1], vamos a denotar
$$A_n = \left\{a + \sqrt{n}b : a, b \in \mathbb{Z}\right\}.$$
Probar las siguientes afirmaciones:
   (i) A_n es un subanillo unitario de $\mathbb{C}$.
   (ii) La *aplicación* $\varphi : A_n \to A_n, a+\sqrt{n}b \mapsto a-\sqrt{n}b$ *conjugación* es un homomorfismo de anillos unitario, mientras que la *aplicación* $N : A_n \to \mathbb{N}, z \mapsto |z\varphi(z)|$ *norma* es multiplicativa.
   (iii) $A_n^* = \{z \in A_n : N(z) = 1\}$,
   (iv) Dado $z \in A_n$ con $N(z) = p$ primo, entonces z es irreducible.
   (v) Sea $p \notin \mathrm{Im}(N)$ un número primo. Si $z \in A_n$ cumple que $N(z) = p^k$, $k = 2, 3$; entonces z es irreducible. ¿Qué sucede para $k > 4$?
   Vamos ahora a centrarnos en el estudio de unos casos concretos.
   (vi) Encontrar $z \in A_6^* \backslash \{\pm 1\}$.
   (vii) Estudiar si $2, 3 \in A_6$ son irreducibles.
   (viii) Determinar cuántos homomorfismos de anillos unitarios $f\colon A_2 \longrightarrow A_3$ existen.
2. Sea $A \subseteq \mathbb{C}$ un subanillo unitario cerrado para la conjugación. Probar las siguientes afirmaciones:
   (i) $A^* = \{z \in A : |z|^2 \equiv z\bar{z} = 1\}$,
   (ii) Si $z \in A$ cumple que $|z|^2 = p$, donde p es un entero primo, entonces z es irreducible.
   (iii) Sea p un número primo tal que $|z|^2 \neq p$ para todo $z \in A$. Si $w \in A$ satisface que $|w|^2 = p^k$, para $k = 2, 3$; entonces w es irreducible.
3. Dado $\varphi\colon A \longrightarrow B$ un isomorfismo de anillos, demostrar que $a \in A$ es irreducible si, y sólo si, lo es $\varphi(a) \in B$. ¿Es esto cierto si φ es simplemente homomorfismo de anillos?
4. (i) Probar que 3 es irreducible, pero no primo, en A_{-5}.
   (ii) Probar que 2 es irreducible, pero no primo, en A_{-3}.
5. En el anillo de los enteros de Gauss,
   (i) Demostrar que un número primo impar p es suma de dos cuadrados si, y sólo si, es reducible (es decir, no es irreducible).
   (ii) Descomponer $3 + i$ y $4 + 3i$ como producto de factores irreducibles.
6. Estudiar cuales son los elementos irreducibles de $\mathbb{Z}/n\mathbb{Z}$ para $n > 2$.

DIPs y DFUs. MCD y MCM.

7. Sean A y B anillos conmutativos.
   (i) Demostrar que, si todos los ideales de A son principales y existe un homomorfismo $f : A \to B$ sobreyectivo, entonces todos los ideales de B son principales. ¿Es necesaria la condición de sobreyectividad?

[1] Un número $n \in \mathbb{Z}$ se dice *libre de cuadrados* si, para todo primo $p \in \mathbb{N}$ tal que $p|n$, se tiene que $p^2 \nmid n$.

(ii) Concluir del apartado anterior que todos los posibles cocientes $A/\mathfrak{a}$ de un anillo conmutativo A, cuyos ideales son principales, satisface que sus ideales también son principales.

8. (i) ¿Es el anillo A_{-5} un DIP? Estudiar si el ideal $(2+i\sqrt{5},3)A_{-5}$ es principal o no.
   (ii) ¿Es el anillo A_{-1} un DIP? Estudiar si el ideal $(5,3+i4)A_{-1}$ es principal o no.
9. En el anillo A_{-26},
   (i) calcular las unidades.
   (ii) estudiar si los elementos $3, 1+i\sqrt{26}$ y $1-i\sqrt{26}$ son irreducibles.
   (iii) estudiar si estamos ante un DFU.
10. El objetivo final de este ejercicio es demostrar que A_n nunca puede ser DFU para todo $n<2$. Para ello, los pasos que se van a seguir son los siguientes:
    (i) Demostrar que el ideal $2A_n \subseteq A_n$ no es primo.
    (ii) Demostrar que, si $n<-2$, entonces no existe ningún elemento $z \in A_n$ tal que $N(z)=|z|^2=2$.
    (iii) Concluir que si $n<-2$ entonces A_n no es un DFU.
11. Probar que 6 y $2+2\sqrt{-5}$ no tienen máximo común divisor en A_{-5}. ¿Qué resultado, ya conocido, podemos concluir?
12. Dar un ejemplo de DFU que no sea DIP.
13. Demostrar que en un DIP dos ideales son comaximales[2] si, y sólo si, un máximo común divisor de sus generadores es 1 (en cuyo caso, se dice que estos son *coprimos*).
14. Sean A un DFU y $x,y,z \in A$ tales que x e y son coprimos con $zn=xy$ para cierto entero positivo n. Demostrar que existen elementos $a,b \in A$ y unidades $u,v \in A^*$ de forma que $x=ua^n$ e $y=vb^n$.

DEs. Algoritmo de Euclídes. Ecuaciones Diofánticas. Sistemas de Congruencias.

15. Demostrar que todo DE es un DIP.
16. Probar que A_2, A_3, A_{-1} y A_{-2} son DEs.
17. El objetivo final de este ejercicio es concluir que un DE es de hecho un cuerpo si, y sólo si, la aplicación que dota de esta estructura es constante. Para ello, se tienen los enunciados siguientes:
    (i) Sean $\mathbb{K}$ un cuerpo y $\varphi : \mathbb{K}\backslash\{0\} \to \mathbb{N}$ una aplicación constante arbitraria. Probar que φ dota a $\mathbb{K}$ con una estructura de DE.
    (ii) Sean $\mathbb{K}$ un cuerpo y $\varphi : \mathbb{K}\backslash\{0\} \to \mathbb{N}$ una función que dote a $\mathbb{K}$ de estructura de DE. Demostrar que φ es constante.
    (ii) Sean A un dominio conmutativo unitario que no es un cuerpo y $\varphi : A\backslash\{0\} \to \mathbb{N}$ una aplicación que dota a A de estructura de DE. Probar que φ no es constante.
18. Sean $\rho = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ y
$$\mathbb{Z}[\rho] = \{a+\rho b : a,b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$
    (i) Demostrar que $N : \mathbb{Z}[\rho]\backslash\{0\} \to \mathbb{N}, a+\rho b \mapsto a^2+b^2-ab$ (*aplicación norma*) dota a $\mathbb{Z}[\rho]$ con una estructura de DE. Calcular las unidades de $\mathbb{Z}[\rho]$.
    (ii) Encontrar un elemento irreducible $z=a+\rho b \in \mathbb{Z}[\rho]$ con $ab \neq 0$ de forma que $N(z)$ no sea un número primo.
    (iii) Demostrar que el ideal generado por $1-\rho$ es maximal.
    (iv) Factorizar 3 como producto de irreducibles en $\mathbb{Z}[\rho]$.
    (v) Demostrar que el cuerpo $\mathbb{Z}[\rho]/(1-\rho)\mathbb{Z}[\rho]$ es finito y calcular su cardinal.
19. Sean $m=17^{13}$ y $n=13^{17}$. Calcular la cifra de las unidades del número 17^m-3^n.

[2]Dos *ideales* $\mathfrak{a}$ y $\mathfrak{b}$ de un anillo A se dicen *comaximales* si $\mathfrak{a}+\mathfrak{b}=A$.

20. Comprobar que
$$a = 6003722857 \text{ y } n = 77695236973$$
son coprimos, y obtener el inverso de a módulo n.
21. (i) Resolver en $\mathbb{Z}[i]$ la ecuación
$$(5-16i)x + (13-10i)y = -1+5i.$$
(ii) Calcular $\mathrm{mcd}(5+2i, 2-i)$ y $\mathrm{mcd}(17, 10+11i)$ en $\mathbb{Z}[i]$. Encontrar una Identidad de Bézout en ambos casos.
22. Resolver en $\mathbb{Z}$ las siguientes ecuaciones:
(i) 25x+40y=24,
(ii) 48x+30y=12,
(iii) 31x+17y=12.
23. El objetivo que nos proponemos es resolver la ecuación diofántica
$$x^3 = y^2 + 2.$$
Para ello, los pasos que se van a seguir son los siguientes:
(i) Probar que, si existen $x, y \in \mathbb{Z}$ satisfaciendo la igualdad anterior, entonces estos enteros son impares y coprimos.
(ii) Demostrar que, si $y \in \mathbb{Z}$ es impar, entonces $y + \sqrt{-2}$ e $y - \sqrt{-2}$ son coprimos en el anillo A_{-2}.
(iii) Demostrar que, para $y, a, b \in \mathbb{Z}$ tales que $y + \sqrt{-2} = (a + \sqrt{-2}b)^3$, se tiene necesariamente que $y = \pm 5$.
(iv) Calcular todas las soluciones enteras de la ecuación $x^3 = y^2 + 2$.
24. El objetivo que nos proponemos es resolver la ecuación diofántica
$$1 + x^2 = 2y^3.$$
Para ello, los pasos que se van a seguir son los siguientes:
(i) Demostrar que toda unidad de $\mathbb{Z}[i]$ es el cubo de otra unidad de $\mathbb{Z}[i]$.
(ii) Dado un entero impar $x \in \mathbb{Z}$, calcular $d = \mathrm{mcd}(x+i, x-i)$ en $\mathbb{Z}[i]$. Demostrar que $d\bar{d} = 2$.
(iii) Encontrar todas las soluciones enteras de $1 + x^2 = 2y^3$.
25. Encontrar las soluciones (si existen) de los siguientes sistemas de congruencias:

(i) $\begin{cases} x \equiv 2 \pmod 7; \\ x \equiv 8 \pmod{15}. \end{cases}$

(ii) $\begin{cases} x \equiv 1 \pmod{11}; \\ x \equiv 12 \pmod{24}; \\ x \equiv 3 \pmod{25}. \end{cases}$

(iii) $\begin{cases} x \equiv 18 \pmod 7; \\ x \equiv 3 \pmod{12}; \\ x \equiv 7 \pmod 5; \\ x \equiv 11 \pmod{28}. \end{cases}$

(iv) $\begin{cases} 6x \equiv 8 \pmod{14}; \\ 9x \equiv 36 \pmod{48}. \end{cases}$

(v) $\begin{cases} x \equiv 6 \pmod{16}; \\ x \equiv 72 \pmod{89}; \\ x \equiv 3 \pmod{23}. \end{cases}$

(vi) $\begin{cases} x \equiv 63 \pmod{91}; \\ x \equiv 23 \pmod{43}; \\ x \equiv 1 \pmod{59}. \end{cases}$

26. Sabemos que el cometa Halley se aproxima a la Tierra con una periodicidad de 76 años, habiéndolo hecho por última vez en el año 1986. Por otro lado, el cometa Temple-Tuttle pasa junto a la Tierra cada 33 años, y la última visita fue en 1998. ¿En qué año se podrá ver a ambos cometas acercarse juntos a la Tierra? Si el cometa Hale-Bopp pasó junto a la tierra en 1997 y su anterior aproximación data del año 2214 a.C., ¿coincidirán alguna vez en nuestro cielo los tres cometas? ¿Se podrán ver alguna vez en años consecutivos? (al hallar el periodo del cometa Hale-Bopp, tener en cuenta que en nuestro calendario no existe el año cero).