Ejercicios de Álgebra Básica. Curso 2018/19

Tema 3: El anillo de los números enteros

Anillos e ideales

Ejercicio 1.– Si X es un conjunto y A es un anillo, entonces A^X tiene una estructura natural de anillo. Además, si A es conmutativo, A^X también es conmutativo.

Ejercicio 2.– Sea X un conjunto no vacío. Definamos dos operaciones sobre el conjunto $\mathscr{P}(X)$ de las partes de X:

$$A + B := A \triangle B = (A \cup B) \setminus (A \cap B), \quad A \cdot B = A \cap B, \quad \forall A, B \in \mathscr{P}(X).$$

Probar que la aplicación biyectiva natural $\alpha : \mathscr{P}(X) \longrightarrow (\mathbb{F}_2)^X$ del ejercicio 26 del Tema 1, definida por

$$\alpha(A)(x) = \begin{cases} \overline{1} & \text{if} \quad x \in A \\ \overline{0} & \text{if} \quad x \notin A, \end{cases}$$

verifica lo siguiente:

$$\alpha(A + B) = \alpha(A) + \alpha(B), \quad \alpha(A \cdot B) = \alpha(A) \cdot \alpha(B), \quad \forall A, B \in \mathscr{P}(X).$$

Concluir primero que $(\mathscr{P}(X), +, \cdot)$ es un anillo conmutativo, y segundo que α es un isomorfismo de anillos. Comprobar además que $A^2 = A$ y que $2A = 0_{\mathscr{P}(X)}$ para todo $A \in \mathscr{P}(X)$.

Ejercicio 3.– Una anillo R se dice *Booleano* si $x^2 = x$ para todo $x \in R$. Si R es un anillo Booleano probar que $2x = 0$ para todo x y que R es conmutativo.

Ejercicio 4.– Probar que el conjunto $R = \left\{ \frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N} \right\} \subset \mathbb{Q}$ es un subanillo conmutativo y unitario. Calcular el conjunto R^* de las unidades de R.

Ejercicio 5.– Sea R un anillo conmutativo e $I, J \subset R$ ideales de R.

1) Probar que $I \cap J$ es también un ideal de R.
2) Definimos la *suma* de I y J como: $I + J := \{x \in R \mid \exists a \in I, \exists b \in J \text{ t.q. } x = a + b\}$. Probar que $I + J$ es un ideal de R.

Ejercicio 6.– Sea R un anillo unitario. Supongamos que $x \in R$ es un elemento con un *único inverso a la izquierda*, es decir, $y \in R$ es el único tal que $yx = 1$. Probar que entonces $xy = 1$ y que, por tanto, x es unidad. (Indicación: considerar el elemento $xy - 1 + y$.)

Ejercicio 7.– Sean I y J dos ideales de un anillo R tales que $I \cap J = \{0\}$. Probar que $xy = 0$ para todos $x \in I$ e $y \in J$.

Ejercicio 8.– Encontrar los divisores de cero de los siguientes anillos: $\mathbb{Z}/\mathbb{Z}15$, $\mathbb{F}_2[x]$ y $\mathbb{Z}/\mathbb{Z}4[x]$.

Ejercicio 9.– Sean I y J dos ideales no nulos de un dominio de integridad. Probar que $I \cap J \neq \{0\}$.

Ejercicio 10.– Probar que el conjunto $R = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \notin \mathbb{Z}2 \right\} \subset \mathbb{Q}$ es un subanillo conmutativo de $\mathbb{Q}$. Calcular el conjunto R^* de las unidades de R. ¿Cuáles son los ideales maximales de R?

Ejercicio 11.– Sea $(V, +)$ un grupo abeliano. Sabemos que V^V tiene una estructura de natural de grupo, que también es abeliano:

$$\text{dados} \quad f, g \in V^V, \quad f + g : V \to V, \quad (f + g)(x) := f(x) + g(x) \quad \forall x \in V.$$

Denotemos por $\mathrm{End}(V)$ al conjunto de los endomorfismos de $(V, +)$, i.e.

$$\mathrm{End}(V) = \{f \in V^V \mid f(x + y) = f(x) + f(y) \ \forall x, y \in V\}.$$

-) Probar que $\mathrm{End}(V)$ es un subgrupo (aditivo) de $(V^V, +)$.
-) Probar que $(\mathrm{End}(V), +, \circ)$ es un anillo ($\circ$ es la composición).

Ejercicio 12.– Denotemos $\mathrm{GL}(n, \mathbb{F}_p)$ el grupo de las matrices $n \times n$ invertibles (o no singulares) con coeficientes en el cuerpo $\mathbb{F}_p$. Estudiar dicho grupo para valores pequeños de p y n.

Divisibilidad en $\mathbb{Z}$

Ejercicio 13.– Probar que para todo número n, n y $n+1$ son primos entre sí.

Ejercicio 14.– Probar que $\mathrm{mcd}(a,m)|\,\mathrm{mcd}(ab,m)$ para cualesquiera enteros a,b,m.

Ejercicio 15.– Probar que si $\mathrm{mcd}(a,b)=1$ y c divide a a, entonces $\mathrm{mcd}(c,b)=1$.

Algoritmo de Euclides. Identidad de Bézout

Ejercicio 16.– Calcular el máximo común divisor, el mínimo común múltiplo y la identidad de Bézout de:

(1). 1520 y 23532.

(2). 1876 y 365.

(3). 5328 y 245.

(4). 600 y 11312.

Ejercicio 17.– Sean a y b enteros con $b>0$. Probar que existen emteros $u,v\in\mathbb{Z}$ tales que $a=bu+v$ con $-\frac{b}{2}\leq v<\frac{b}{2}$. (Indicación: comenzar con el algoritmo de división).

Ejercicio 18.– Probar que $\mathrm{mcd}(2n+6,n^2+3n+2)=2$ o 4 para cualquier entero n, y que ambas posibilidades pueden ocurrir.

Ejercicio 19.– Sean $a,b,c\in\mathbb{Z}$. Probar que si $\mathrm{mcd}(a,b)=1$, $a|c$ y $b|c$ entonces $ab|c$.

Ejercicio 20.– Probar que $6|n^3-n$ para todo $n\in\mathbb{Z}$.

Ejercicio 21.– Probar que 6 divide a $n(n+1)(2n+1)$ para todo n natural.

Ejercicio 22.– Demostrar los siguientes resultados:

(1). Para cualesquiera $a,b,c\in\mathbb{Z}$ se verifica $c\cdot\mathrm{mcd}(a,b)=\mathrm{mcd}(ac,bc)$.

(2). Sean $a,b,d,\alpha,\beta\in\mathbb{Z}$, si $\mathrm{mcd}(a,b)=d$ y $\alpha a+\beta b=d$ entonces $\mathrm{mcd}(\alpha,\beta)=1$.

(3). Si a,b,c son enteros tales que $a|bc$ y $\mathrm{mcd}(a,b)|c$ entonces $a|c^2$.

(4). Si a y b son enteros primos entre sí entonces también lo son $a+b$ y $(a+b)^2+ab$.

Ejercicio 23.– Demostrar que la fracción $(2n+3)/(4n+5)$ es irreducible para todo n natural.

Ejercicio 24.– Sean $a=n^3+3n^2-7,\ b=n+1$ dos números enteros con $n>2$. Demostrar que todo divisor común de a y b divide a 5.

Ejercicio 25.– Demuestre que si $p>0$ es un primo, entonces $\sqrt{p}$ no es racional.

Ejercicio 26.– Probar que para cualesquiera enteros a,b,c, si a divide a bc, entonces $a/\mathrm{mcd}(a,b)$ divide a c.

Ejercicio 27.– Sean $a,b,c\in\mathbb{Z}$. Probar que si $\mathrm{mcd}(a,b)=1$, entonces $\mathrm{mcd}(ac,bc)=c$.

Ejercicio 28.– Responder a las siguientes cuestiones:

(1). Sean $a,b,c\in\mathbb{N}$. Probar que si $\mathrm{mcd}(a,b)=1$ y $ab=c^2$, entonces existen $n,m\in\mathbb{N}$ tales que $a=n^2$, $b=m^2$. (Probar que si p es primo con $p|a$ entonces $p^2|a$.)

(2). Probar que si $\mathrm{mcd}(a,b)=1$, entonces $\mathrm{mcd}(a+b,a-b)=1$ o 2.

(3). Si al aplicar el algoritmo de Euclides para calcular el $\mathrm{mcd}(a,b)$ se obtiene un resto que es un número primo p, probar que $\mathrm{mcd}(a,b)=1$ o p.

Ejercicio 29.– Probar que $\mathrm{mcd}(a,b)=1$ si y sólo si $\mathrm{mcd}(a,b^r)=1$, para todo natural r.

Ejercicio 30.– Probar que si $m|a-b$ y $m|c-d$ entonces $m|ac-bd$. Probar que si $a\equiv b \pmod m$ entonces $a^n\equiv b^n \pmod m$, para todo $n\in\mathbb{N}$.

Ejercicio 31.– Probar que si $a\equiv b \pmod r$ y $a\equiv b \pmod s$ entonces $a\equiv b \pmod{\mathrm{mcm}(r,s)}$.

Ejercicio 32.– Sean a,b,m,r enteros positivos, $d=\mathrm{mcd}(r,m)$. Probar que si $ra\equiv rb \pmod m$ entonces $a\equiv b \pmod{m/d}$.

Ejercicio 33.– Probar que si $x\equiv y \pmod m$ entonces $\mathrm{mcd}(x,m)=\mathrm{mcd}(y,m)$.

Ejercicio 34.– Probar que si $ra\equiv rb \pmod{rm}$ entonces $a\equiv b \pmod m$.

Ejercicio 35.– Probar que para cualesquiera enteros a,b,m, se verifica que $\mathrm{mcd}(ab,m)$ divide a $\mathrm{mcd}(a,m)\cdot\mathrm{mcd}(b,m)$ (usar Bézout). Probar que si a y b son primos entre sí, entonces $\mathrm{mcd}(ab,m)=\mathrm{mcd}(a,m)\cdot\mathrm{mcd}(b,m)$. (Usar ejercicio 19)

Ejercicio 36.– Razone si las siguientes afirmaciones son verdaderas o falsas.

(1). Dados a, $b\in\mathbb{Z}$, si existen α y $\beta\in\mathbb{Z}$ tales que $\alpha a+\beta b=2$, entonces $2|\mathrm{mcd}(a,b)$.

(2). Dados a, $b\in\mathbb{Z}$ com $\mathrm{mcd}(a,b)=d$, para todo α, $\beta\in\mathbb{Z}$ se tiene que $\alpha a+\beta b$ es un múltiplo de d.

Ejercicio 37.– Demuestre que $n(n+1)(n^2+n+1)$ es divisible por 6 para todo natural $n\in\mathbb{N}$.

Ejercicio 38.–

(1). Demuestre que un número congruente con 2 módulo 3 tiene en su descomposición algún primo congruente con 2 módulo 3. Indicación: si $n=p_1^{r_1}\dots p_s^{r_s}$ es la factorización en factores primos de n, ¿qué pasaría si todos los factores primos no son congruentes con 2 módulo 3?

(2). Deduzca que hay infinitos primos de la forma $3n+2$. Indicación: usar la estrategia de la demostración de Euclides de que existen infinitos primos.

Ejercicio 39.– En $\mathbb{Z}/\mathbb{Z}24$ calcular los inversos multiplicativos de $7+\mathbb{Z}24$ y de $13+\mathbb{Z}24$,

Ejercicio 40.– Resolver, si es posible, las siguientes ecuaciones en congruencias:

(1). $13x\equiv 5 \pmod{11}$

(2). $8x\equiv 20 \pmod{12}$

(3). $8x\equiv 5 \pmod{10}$

(4). $28x\equiv 36 \pmod{24}$

Ejercicio 41.– Resolver los siguientes sistemas

(1). $\begin{cases} x\equiv 5 \mod 2\\ x\equiv 6 \mod 3\\ x\equiv 7 \mod 5\\ x\equiv 8 \mod 7\end{cases}$

(2). $\begin{cases} x\equiv 33 \mod 63\\ x\equiv 32 \mod 64\\ x\equiv 34 \mod 65\end{cases}$

(3). $\begin{cases} x\equiv 18 \mod 11\\ x\equiv 3 \mod 18\\ x\equiv 7 \mod 25\\ x\equiv 11 \mod 7\end{cases}$

(4). (Yih − hing, 717 a.C.) $\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 5 \\ x \equiv 5 \mod 6 \\ x \equiv 5 \mod 12 \end{cases}$

Ejercicio 42.– Sean a, b y c enteros no nulos; demuestre que

$$\text{la ecuación } ax + by = c \text{ tiene solución entera} \iff \text{mcd}(a, b)|c.$$

Ejercicio 43.– Encontrar todas las soluciones enteras de la ecuación $6x + 11y = 1$,

Ejercicio 44.– Cinco piratas intentan repartirse una bolsa de monedas de oro del útimo botín y sobran tres monedas. Poco después, el capitán de los piratas descubre que el timonel y el cocinero se querían quedar con otra bolsa igual que la primera y les obliga a compartir su bolsa. Ahora, después de repartir las monedas de oro de las dos bolsas entre los cinco piratas, el timonel y el cocinero, sobran cuatro monedas. ¿Cuántas monedas tiene cada bolsa si hay entre 100 y 150 monedas por bolsa?

Ejercicio 45.– Cuál es el menor número de huevos que una cesta puede contener si, tomados de k en k queda un huevo en la cesta cuando $k = 2, 3, 4, 5, 6$ y ningún huevo cuando $k = 7$. (Este problema aparece en un manuscrito de la India del siglo VII).

Ejercicio 46.– En cierta cultura se celebran los festivales de la serpiente, el mono y el pez cada 6, 5 y 11 años respectivamente. Los próximos festivales serán dentro de 3, 4 y 1 año respectivamente. ¿Cuántos años deben pasar para que todos los festivales se celebren el mismo año?

Ejercicio 47.– Un niño piensa repartir en su cumpleaños una bolsa de caramelos entre sus cinco amigos y sabe que sobrarán dos caramelos. Al final, van también sus seis primos y le gustaría repartir caramelos entre once niños. Como son más niños de los previstos sus padres le dan más caramelos, de manera que tiene el doble de antes más diez. Ahora le sobran ocho. ¿Cuántos caramelos tenía en la bolsa al principio sabiendo que la bolsa tenía menos de 80 caramelos?

Los teoremas de Fermat y de Euler

Ejercicio 48.– Calcular las unidades de $\mathbb{Z}/\mathbb{Z}11$ y $\mathbb{Z}/\mathbb{Z}16$.

Ejercicio 49.– Demostrar los siguientes resultados:

(1). Si a es primo con 2 y 3, $(a^2 - 1)$ es divisible por 24. (Usar el ejercicio 19)

(2). $n^{13} - n$ es divisible entre $2, 3, 5, 7, 13$ para cualquier entero n.

(3). Los enteros a y a^5 tienen igual el último dígito en base 10.

(4). Si $n > 2$ es impar y el orden de 2 en $\mathbb{Z}/\mathbb{Z}n$ es $n - 1$, entonces n es primo.

(5). Probar que para todo $n \in \mathbb{Z}$ el número $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ es entero.

(6). Probar que para todo $n \in \mathbb{Z}$ el número $n^9 + 2n^7 + 3n^3 + 4n$ es múltiplo de 5.

(7). Probar que $n^{111} \equiv n \pmod{11}$, para todo $n \in \mathbb{Z}$.

Ejercicio 50.– Sea p un número primo distinto de 2 y 5. Probar que p divide a uno de elementos del conjunto $\{1, 11, 111, 1111, ...\}$. (Usar que $(10^n - 1)/9 = 11 \ldots 1$.)

Ejercicio 51.– Demuestre que para todo $n \in \mathbb{N}$ se tiene que $n^7 - n$ es múltiplo de 7.

Ejercicio 52.– Calcular el resto de dividir 12^{39} entre 13. Idem con 6^{37}.

Ejercicio 53.– ¿Es $2222^{5555} + 5555^{2222}$ divisible por 7? ¿es $4444^{3333} + 3333^{4444}$ divisible por 7?