

Primera serie de ejercicios de Álgebra Moderna

Akiyuki Shinbou

Mayo 2018

Problema 1. Para $n = 5, 8, 12, 20$ y 25 , encuentra todos los enteros positivos menores a n y relativamente primos a n .

Solución:

Para $n = 5$: $\{1, 2, 3, 4\}$

Para $n = 8$: $\{1, 3, 5, 7\}$

Para $n = 12$: $\{1, 5, 7, 11\}$

Para $n = 20$: $\{1, 3, 7, 9, 11, 13, 17, 19\}$

Para $n = 25$: $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$

Problema 2. Determina $\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11)$ y $\text{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11)$

Solución:

$$\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11) = 2 \cdot 3^2 \cdot 7.$$

$$\text{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11) = 2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$$

Problema 3. Determine $51 \bmod 13$, $342 \bmod 85$, $62 \bmod 15$, $10 \bmod 15$, $(82 \cdot 73) \bmod 7$, $(51 + 68) \bmod 7$, $(35 \cdot 24) \bmod 11$, y $(47 + 68) \bmod 11$.

Solución:

$$51 \bmod 13 = 12$$

$$342 \bmod 85 = (2 \bmod 85 \cdot 171 \bmod 85) \bmod 85 = (2 \cdot 1) \bmod 85 = 2$$

$$62 \bmod 15 = 2$$

$$10 \bmod 15 = 10$$

$$(82 \cdot 73) \bmod 7 = (5 \cdot 3) \bmod 7 = 1$$

$$(51 + 68) \bmod 7 = (2 + 5) \bmod 7 = 0$$

$$(35 \cdot 24) \bmod 11 = (2 \cdot 2) \bmod 11 = 4$$

$$(47 + 68) \bmod 11 = (3 + 2) \bmod 11 = 5$$

Problema 4. Encuentra enteros s y t tales que $1 = 7 \cdot s + 11 \cdot t$. Muestra que s y t no son unicos.

Solución:

Dos soluciones: $s = 8, t = -5$; $s = 19, t = -12$

Problema 5. En Florida, el cuarto y quinto dígito del final de una licencia de conducir da el año de nacimiento. Los últimos tres dígitos de un hombre con mes de nacimiento m y día de nacimiento b son representados por $40(m - 1)$. Para las mujeres los dígitos son $40(m - 1) + b + 500$. Determine las fechas de nacimiento y sexos correspondientes a los números 42218 y 53953.

Solución:

42218: Hombre; 18 de Junio del 42.

53953: Mujer; 13 de diciembre del 53.

Problema 6. Para las licencias de conducir en Nueva York previas al septiembre de 1992, los tres dígitos precediendo a los últimos 3 del número de un hombre con mes de nacimiento m y día de nacimiento b se representan por $63m + 2b$. Para mujeres los dígitos son $63m + 2b + 1$. Determine las fechas de nacimiento y los sexos correspondientes a los números 248 y 601.

Solución:

248: Mujer; 29 de Junio.

601: Hombre; 17 de Septiembre

Problema 7. Demuestra que si a y b son enteros positivos, entonces $ab = \text{lcm}(a, b) \cdot \text{gcd}(a, b)$.

Solución:

Podemos expresar a y b como factores primos elevados a una potencia no negativa: $a = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_k^{m_k}$ y $b = p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_k^{n_k}$. Entonces $\text{lcm}(a, b) = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_k^{s_k}$, donde $s_i = \max(m_i, n_i)$ y $\text{gcd}(a, b) = p_1^{t_1} \cdot p_2^{t_2} \cdot \dots \cdot p_k^{t_k}$ donde $t_i = \min(m_i, n_i)$. Ahora, $\text{lcm}(a, b) \cdot \text{gcd}(a, b) = p_1^{m_1+n_1} \cdot p_2^{m_2+n_2} \cdot \dots \cdot p_k^{m_k+n_k} = ab$.

Problema 8. Supón que a y b son enteros que dividen al entero c . Si a y b son primos relativos, demuestra que ab divide a c . Muestra, por ejemplo, que si a y b no son primos relativos, entonces ab no necesariamente divide a c .

Solución:

Si a y b son primos relativos, entonces los podemos expresar como una relación lineal $1 = as + bt$. Además, como a y b dividen a c , sabemos que existen $u, v \in \mathbb{Z}$ tales que $c = ua$ y $c = vb$. Procede que $c = cas + cbt = vbas + uabt = ab(vs) + ab(ut) = ab(vs + ut)$, es decir, ab divide a c .

Para el contraejemplo tomamos $a = 6$, $b = 4$ y $c = 12$. 6 y 4 no son primos relativos y dividen a 12, sin embargo $6 \cdot 4 = 24$ no divide a 12.

Problema 9. Si a y b son enteros y n es un entero positivo, pruebe que $a \bmod n = b \bmod n$ si y solo si n divide $a - b$

Solución:

Para probar esto, empecemos por demostrar que:

Si $a \bmod n = b \bmod n$ entonces $a - b \bmod n = 0$.

A partir de la hipótesis:

$a \bmod n - b \bmod n = 0$, y aplicando división modular por ambos lados obtenemos:

$$(a \bmod n - b \bmod n) \bmod n = 0 \bmod n$$

Y haciendo un breve desarrollo de la ecuación que buscamos encontrar:

$$a - b \bmod n = (a \bmod n - b \bmod n) \bmod n$$

Se realiza exactamente lo mismo para demostrar que la proposición es bicondicional.

Problema 10. Sean a y b enteros y $d = \gcd(a, b)$. Demuestre que si $a = da'$ y $b = db$, entonces $\gcd(a', b') = 1$.

Solución:

Sabemos que existen $s, t \in \mathbb{Z}$ tales que $d = as + bt = (da')s + (db')t = d(sa' + tb')$. Dividiendo ambos lados por d tenemos que $1 = sa' + tb'$. Regresándonos a la definición, si decimos que $d' = \gcd(a', b')$, entonces $d' | a'$ y $d' | b'$, entonces $d' | tb' + sa'$. Así, $d' | 1$ lo que significa que $d' = 1$.

Problema 12. Sean a y b enteros positivos y sea $d = \gcd(a, b)$ y $m = \text{lcm}(a, b)$. Demuestre que si t divide a a y b , t divide a d . Demuestre que si s es un múltiplo de a y b , s es un múltiplo de m .

Solución:

Suponiendo que t divide a a y b . Existe enteros x, y tales que $ax + by = t$. Porque t divide a a y b , también cualquier combinación lineal de a y b , por tanto t divide a d .

Suponiendo que s es múltiplo de a y b . Por el algoritmo de la división, existe un $0 \leq r < m$ y q tal que: $S = mq + r$, esto implica que: $r = s - mq$.

s es un común múltiplo de a y b , y m es un común múltiplo. Pero $0 \leq r < m$ y porque m es el mínimo común múltiplo, entonces $r = 0$. Por lo tanto $s = mq$

Problema 13. Sean n y a enteros positivos y $d = \gcd(a, n)$. Demuestre que la ecuación $ax \pmod n = 1$ tiene una solución si y solo si $d = 1$.

Solución:

$$\begin{aligned} ax &= nk + 1, d > 1 \\ \frac{ax}{d} &= \frac{nk + 1}{d} \\ \frac{ax}{d} &= \frac{nk}{d} + \frac{1}{d} \\ a'x &= n'k + \frac{1}{d} \end{aligned}$$

Esto significa que el modulo de la operacion es $\frac{1}{d}$ y la unica forma que eso sea 1, es si $d = 1$.

Problema 15. Demuestra que todo primo mayor a 3 puede ser escrito de la forma $6n + 1$ o $6n + 5$.

Solución:

Considerando los residuos posibles al dividir un primo entre 6, observamos que el residuo no puede ser 0, 2 o 4, porque significaría que el numero es divisible por 2. No puede ser 3, porque implicaría que el numero es divisible entre 3. Esto nos deja con $6n + 1$ y $6n + 5$ como las formas que podrian representar un numero primo.

Problema 16. Determina $7^{1000} \pmod 6$ y $6^{1001} \pmod 7$.

Solución:

Considerando que $a \cdot b \pmod n = a \pmod n \cdot b \pmod n$, podemos notar que la primer división nos resulta 1, ya que $7 \pmod 6 = 1$. Mientras que, por otra parte, $6 \pmod 7 = 6$, por lo que la segunda división debemos resolverla a partir de una observación adicional. Notemos que $36 \pmod 7 = 1$ y que $6 \cdot 36 \pmod 7 = 6$, por la propiedad antes mencionada. Lo que significa que podemos resumirlo como $6^n \pmod 7 = 1$ si $n \pmod 2 = 0$, y $6^n \pmod 7 = 6$ si $n \pmod 2 = 1$, entonces $6^{1001} \pmod 7 = 6$.

Problema 17. Sean a, b, s y t enteros. Si $a \pmod s = b \pmod s$, demuestra que $a \pmod s = b \pmod s$ y $a \pmod t = b \pmod t$. ¿Cual es la condicion de s y t

que hacen que lo opuesto sea verdad?

Solución:

a y b dejan el mismo residuo al ser divididos por st. Es posible entonces expresar $a = st \cdot q_1 + r$ y $b = st \cdot q_2 + r$. Como a y b son divisibles por st y st es divisible por s entonces r es dividido por s por lo que $r = s \cdot q_3 + r_s$ con $0 \leq r_s < s$. De esta forma $a = st \cdot q_1 + s \cdot q_3 + r_s$ y $b = st \cdot q_2 + s \cdot q_3 + r_s$. Reordenando:

1. $a = s(tq_1 + q_3) + r_s$

2. $b = s(tq_2 + q_3) + r_s$

Lo anterior es posible traducirse como que a y b dejan el mismo residuo al ser divididos por s. Con ello $a \bmod s = b \bmod s$.

Un procedimiento análogo se sigue para demostrar que $a \bmod t = b \bmod t$.

La condición necesaria para que se cumpla es que s y t sean primos relativos.

Problema 19. Demuestre que $\gcd(a, bc) = 1$ si y solo si $\gcd(a, b) = 1$ y $\gcd(a, c) = 1$.

Solución:

Si $\gcd(a, bc) = 1$ entonces no existe ningún primo que divida tanto a como a bc. Usando la descomposición en primos y el lema de Euclides, podemos decir que no existe primo que divida tanto a a como a b o a como a c. Por esto, $\gcd(a, b) = 1$ y $\gcd(a, c) = 1$.

Por otro lado, si $\gcd(a, b) = 1$ y $\gcd(a, c) = 1$, entonces no existe primo que divida tanto a como b o a como a c. Por el lema de euclides tambien sabemos que no existe primo que divida tanto a a como a bc, por lo que $\gcd(a, bc) = 1$.

Problema 20. Sean p_1, p_2, \dots, p_n primos. Demuestra que $p_1 p_2 \cdots p_n$ no es divisible por ninguno de estos primos.

Solución:

p_1, p_2, \dots, p_n es divisible por cada numero en la lista, pero si se suma 1, ciertamente seria divisible por algun primo pero no por los primos en la lista. Si 1 fuese primo entonces seria el caso pero no lo es.

Problema 22. Para cada entero positivo n, demuestra que $1 + \cdots + n = n(n+1)/2$.

Solución:

Por inducción. El caso base dice que $1 = 1(1+1) / 2 = 1$.

Para el paso inductivo, asumimos que $1 + \cdots + n = n(n+1)/2$ y queremos

probar que $1 + \cdots + n + n + 1 = (n+1)((n+1)+1)/2$. Sustituyendo la hipótesis obtenemos que $n(n+1)/2 + (n+1) = (n+1)((n+1)+1)/2$

$$\begin{aligned} 1 + \cdots + n + (n+1) &= n(n+1)/2 + (n+1) \\ &= (n(n+1) + 2(n+1))/2 \\ &= (n+2)(n+1)/2 \\ &= (n+1)((n+1)+1)/2 \end{aligned}$$

Problema 23. Para todo entero positivo n , pruebe que un conjunto con exactamente n elementos tiene exactamente 2^n subconjuntos (contando el conjunto vacío y el conjunto mismo).

Solución:

Para esta prueba recurriremos a la inducción matemática. Para el paso base, cuando $n = 1$, tenemos 2 subgrupos, lo cual es correcto, ya que corresponden al conjunto vacío y al conjunto mismo.

Para el paso inductivo, vamos a demostrar que un conjunto con $n + 1$ elementos tiene 2^{n+1} subgrupos, con la hipótesis correspondiente (un conjunto de n elementos tiene 2^n subgrupos).

Para ello, es necesario notar que $2^{n+1} = 2 \cdot 2^n$. Recordemos que por hipótesis 2^n es el número de subgrupos que tiene un conjunto de n elementos. Y si multiplicamos por dos ese número, obtendríamos el total de subgrupos, ya que son los que ya teníamos, más ahora todos esos subgrupos iguales incluyendo al nuevo elemento.

Problema 24. Para todo entero positivo n , demuestre que $2^n 3^{2n} - 1$ siempre es divisible por 17.

Solución:

Por inducción. El caso base dice que $2^1 3^2 - 1 = 17$ es divisible entre 17.

Para el paso inductivo queremos probar que $2^{n+1} 3^{2n+2} - 1$ es divisible entre 17 sabiendo que $2^n 3^{2n} - 1$ es divisible entre 17, digamos $17m = 2^n 3^{2n} - 1$ donde m es un número entero positivo.

$$\begin{aligned}
2^{n+1}3^{2n+2} - 1 &= 2^13^22^n3^{2n} - 1 \\
&= 18(2^n3^{2n}) - 1 \\
&= 18(2^n3^{2n} - 1) - 17 \\
&= 18(17m) - 17 \\
&= 17(18m - 1)
\end{aligned}$$

Problema 26. Demuestra que si p es un primo y p divide a $a_1a_2 \dots a_n$, entonces p divide a a_i para algun i .

Solución:

Inducción sobre n . En el caso base p divide a a_1 por definición.

En el caso inductivo, queremos probar que si p divide a $a_1a_2 \dots a_na_{n+1}$ entonces p divide a algun a_i , sabiendo que p divide a $q = a_1a_2 \dots a_n$ esto se cumple con el lema de euclides, sabiendo que $a_1a_2 \dots a_na_{n+1} = qa_{n+1}$ y que p divide a q .

Problema 27. Utiliza el lema generalizado de Euclides para establecer la parte de unicidad del teorema fundamental de la aritmética.

Solución:

$n = p_1p_2 \dots p_n$. Si p_i divide n , entonces n se reescribe como: $\frac{n}{p_i} = p_i \dots p_{i-1}p_{i+1} \dots p_m$ por lo que se reduce la expresion. Si se repite el proceso, se puede ver que se llega siempre a $\frac{n}{p_1 \dots p_m} = 1$, lo cual muestra la unicidad.

Problema 29. Demuestra que el primer principio de la inducción matemática es una consecuencia del principio del ordenamiento.

Solución:

Tomamos S como un conjunto que contiene al elemento a y siempre que $n \geq a$ pertenece a S , entonces $n + 1 \in S$. Debemos demostrar que S contiene a todos los enteros mayores o iguales a a . Sean T los enteros mayores que a que no se encuentran en T y supongamos que T no está vacío. Sea b el número más pequeño en T , es decir, que $b - 1 \in S$. Si esto es así, entonces $(b - 1) + 1 \in S$, lo cual contradice nuestra suposición que $b \in T$.

Problema 30. Los números de Fibonacci son 1, 1, 2, 3, 5, 8, 13, 21, 34, En general, los números Fibonacci se definen por $f_1 = 1, f_2 = 1$, y para $n \geq 3, f_n = f_{n-1} + f_{n-2}$. Pruebe que el n -ésimo número de Fibonacci f_n satisface $f_n < 2^n$.

Nuevamente utilizaremos inducción matemática para demostrar tal proposición. Nuestro caso base es cuando $n = 3$, quedando de la siguiente manera:

$$\begin{aligned}
f_3 &= 1 + 1 = 2 \\
2 &< 2^3
\end{aligned}$$

Ahora en el paso inductivo, tenemos por hipótesis que $f_n < 2^n$ y vamos a demostrar que $f_{n+1} < 2^{n+1}$

$$f_n + f_{n-1} < 2 \cdot 2^n$$

$$f_n + f_{n-1} < 2^n + 2^n$$

Quedando evidente que se cumple la proposición mencionada.

Problema 31. En la canción “As” de Songs in the Key of Life, Stevie Wonder menciona que la ecuación $8 \times 8 \times 8 \times 8 = 4$. Encuentra todos los enteros para los cuales esto se cumple, modulo n .

Solución:

Se cumple para cualquier divisor de $8^4 - 4 = 4092$.

Problema 33. Si fuesen las 2:00 A.M., ¿que hora sería en 3736 horas?

Solución:

$(2 + 3736) \bmod 24 = 18$ horas, o las 6:00 p.m..

Problema 36. Supón que una un número de identificación de una orden de dinero y dígito de verificación 21720421168 es copiado erróneamente como 27750421168. ¿El dígito de verificación detectará el error?

Solución:

$2172042116 \bmod 9 = 8$ y $2775042116 \bmod 8 = 9$, así que no, el error no será detectado.

Problema 43. El número de libro estándar internacional de 10 dígitos (ISBN-10) $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ tiene la propiedad $(a_1, a_2, \dots, a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \bmod 11 = 0$. El dígito a_{10} es el dígito de verificación. Verifica el dígito para el ISBN-10 asignado a este libro.

Solución:

El ISBN-10 es 0-547-16509-9. $(0, 5, 4, 7, 1, 6, 5, 0, 9, 9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) = 209$. $209 \bmod 11 = 0$

Problema 44. Supón que un ISBN-10 tiene una entrada borrada: 0-716?-2841-9. Determine el dígito faltante.

Solución:

La solución a la ecuación $(0, 7, 1, 6, x, 2, 8, 4, 1, 9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \bmod 11 = 0$ tal que $0 \leq x \leq 9$ es 7.

Problema 50. El estado de Utah anexa un noveno dígito a_9 al número de ocho dígitos de una licencia de conducir $a_1a_2 \dots a_8$ de manera que $(9a_1 + 8a_2 + 7a_3 + 6a_4 + 5a_5 + 4a_6 + 3a_7 + 2a_8 + a_9) \bmod 10 = 0$. Si sabes que el número de licencia tiene exactamente un dígito incorrecto, explica porque el error no puede estar en la posición 2, 4, 6 o 8.

Solución:

Cambiar uno de los dígitos pares hace que al momento de verificar el resultado cambie por una cantidad par, sin embargo $(9 \cdot 1 + 8 \cdot 4 + 7 \cdot 9 + 6 \cdot 1 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 2 + 2 \cdot 6 + 7) \bmod 10 = 5$.

Problema 57. Suponga que α , β y γ son funciones. Si $\alpha\gamma = \beta\gamma$ y γ es uno a uno y sobre, demuestre que $\alpha = \beta$.

Solución:

Si γ es sobre y uno a uno, entonces existe una función inversa γ^{-1} , y multiplicando $\alpha\gamma = \beta\gamma$ por γ^{-1} por el lado derecho obtenemos que $\alpha = \beta$.