Soluciones tema 4: Teoría de números

Ejercicio 1

Encuentre el $mcd(10933, 832)$.

Solución

$$\begin{aligned}
mcd(10933, 832) &= mcd(832, res(10933, 832)) \\
10933 &= 832 \cdot 13 + 117 \rightarrow mcd(832, 117) \\
mcd(832, 117) &= mcd(117, res(832, 117)) \\
832 &= 117 \cdot 7 + 13 \rightarrow mcd(117, 13) \\
mcd(117, 13) &= mcd(13, res(117, 13)) \\
117 &= 13 \cdot 9 + 0 \rightarrow mcd(13, 0) \\
mcd(13, 0) &= 13
\end{aligned}$$

Por tanto: $mcd(10933, 832) = 13$

Ejercicio 2

Considere la siguiente ecuación:

$$13x = 60y + 1.$$

Utilizando el algoritmo del Pulverizador, encuentre la pareja de valores x e y solución de la ecuación con la x positiva más pequeña posible. La variable y puede ser negativa. Tanto x como y deben ser enteros.

Solución

Podemos escribir $13x = 60y + 1$ como $13x - 60y = 1$, dándonos así cuenta de que x e y son una combinación lineal de 1. Planteamos el Pulverizador con $a = 60$ y $b = 13$:

a	b	res	$= a - q \cdot y$
60	13	8	$= 60 - 4 \cdot 13$
13	8	5	$= 13 - 1 \cdot 8 = 13 - 60 + 4 \cdot 13 = -60 + 5 \cdot 13$
8	5	3	$= 8 - 1 \cdot 5 = 60 - 4 \cdot 13 - 5 \cdot 13 + 60 = 2 \cdot 60 - 9 \cdot 13$
5	3	2	$= 5 - 1 \cdot 3 = 5 \cdot 13 - 60 - 2 \cdot 60 + 9 \cdot 13 = -3 \cdot 60 + 14 \cdot 13$
3	2	1	$= 3 - 1 \cdot 2 = 2 \cdot 60 - 9 \cdot 13 + 3 \cdot 60 - 14 \cdot 13 = 5 \cdot 60 - 23 \cdot 13$

Por tanto, tenemos que $x = -23$ e $y = -5$. Como queremos que $x \geq 1$, hacemos la siguiente operación:

Ejercicio 3

Calcule el residuo de $12^{43} \pmod{713}$.

Solución

En primer lugar, descomponemos el exponente (43) en potencias de dos:

$$43 = 2^5 + 2^3 + 2^1 + 2^0 = 32 + 8 + 2 + 1$$

Por tanto:

$$12^{43} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12$$

Recurriendo a ellas, calculamos por fin el residuo de $12^{43} \pmod{713}$.

$$\begin{aligned}
12^2 &= 12^2 = 144 &\pmod{713}\\
12^4 &= (12^2)^2 = 144^2 = 20736 \equiv 59 &\pmod{713}\\
12^8 &= (12^4)^2 \equiv 59^2 = 3481 \equiv 629 &\pmod{713}\\
12^{16} &= (12^8)^2 \equiv 629^2 = 395641 \equiv 639 &\pmod{713}\\
12^{32} &= (12^{16})^2 \equiv 639^2 = 408321 \equiv 485 &\pmod{713}\\
12^{43} &= 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12 \equiv 485 \cdot 629 \cdot 144 \cdot 12 = 527152320 \equiv 48 &\pmod{713}
\end{aligned}$$

Por tanto: $12^{43} \equiv 48 \pmod{713}$

Ejercicio 4

Recurriendo a la aritmética modular, demuestre que $100|(11^{10} - 1)$.

Solución

Operamos utilizando aritmética modular con módulo 100. Podemos resolver el problema de varias formas. Podemos, por ejemplo, calcular el residuo de $11^{10} \pmod{100}$ de forma directa:

$$\begin{aligned}
11^2 &= 11 \cdot 11 = 121 \equiv 21 &\pmod{100}\\
11^3 &= 11^2 \cdot 11 \equiv 21 \cdot 11 = 231 \equiv 31 &\pmod{100}\\
11^4 &= 11^3 \cdot 11 \equiv 31 \cdot 11 = 341 \equiv 41 &\pmod{100}\\
11^5 &= 11^4 \cdot 11 \equiv 41 \cdot 11 = 451 \equiv 51 &\pmod{100}\\
11^6 &= 11^5 \cdot 11 \equiv 51 \cdot 11 = 561 \equiv 61 &\pmod{100}
\end{aligned}$$

También podemos recurrir a las potencias de 2. Pues sabemos que $10 = 8+2$ y, por tanto: $11^{10} = 11^8 \cdot 11^2$. Sabiendo esto, podemos calcular el residuo de 11^{10} (mód 100) de la siguiente forma:

$$\begin{aligned} 11^2 &= 11 \cdot 11 = 121 \equiv 21 \pmod{100} \\ 11^4 &= (11^2)^2 \equiv 21^2 = 441 \equiv 41 \pmod{100} \\ 11^8 &= (11^4)^2 \equiv 41^2 = 1681 \equiv 81 \pmod{100} \\ 11^{10} &= 11^8 \cdot 11^2 \equiv 81 \cdot 21 = 1701 \equiv 1 \pmod{100} \end{aligned}$$

Para ambos casos, como $11^{10} \equiv 1 \pmod{100}$, entonces $(11^{10} - 1) \equiv 0 \pmod{100}$. Es decir, que $100|(11^{10} - 1)$. $\square$

Ejercicio 5

Recurriendo a la aritmética modular, demuestre que $7|(2222^{5555} + 5555^{2222})$.

Solución

Operamos utilizando aritmética modular con módulo 7. En primer lugar, simplificamos las bases de las potencias a su residuo módulo 7:

$$\begin{aligned} 2222 &\equiv 3 \pmod{7} \\ 5555 &\equiv 4 \pmod{7} \\ 2222^{5555} + 5555^{2222} &\equiv 3^{5555} + 4^{2222} \pmod{7} \end{aligned}$$

Por el pequeño teorema de Fermat sabemos que, dado un primo p y un k que no sea múltiplo de p, se cumple que $k^{p-1} \equiv 1 \pmod{p}$. Por tanto, y dado que 7 es un número primo y $k_1 = 3$ y $k_2 = 4$ no son múltiplos de p, entonces se cumple que:

$$\begin{aligned} 3^6 &\equiv 1 \pmod{7} \\ 4^6 &\equiv 1 \pmod{7} \end{aligned}$$

Y como:

$$\begin{aligned} 5555 &= 925 \cdot 6 + 5 \\ 2222 &= 370 \cdot 6 + 2 \end{aligned}$$

Tenemos que:

$$3^{5555} + 4^{2222} = (3^6)^{925} \cdot 3^5 + (4^6)^{370} \cdot 4^2 \pmod{7}$$

Ejercicio 6

Demuestre que $7^{11}|(3^{6\cdot 7^{10}}-1)$.

Solución

Pensamos en el teorema de Euler, que dice que, dados unos k y n primos relativos: $k^{\phi(n)} \equiv 1 \pmod{n}$. Esto mismo, escrito de otra forma:

$$n|(k^{\phi(n)}-1)$$

Nos fijamos en que el divisor es 7^{11}, y aplicamos sobre él la función indicatriz de Euler:

$$\phi(7^{11}) = 7^{11}(1-\frac{1}{7}) = 6\cdot 7^{10}$$

Por tanto:

$$3^{6\cdot 7^{10}} = 3^{\phi(7^{11})}$$

Así que comprobamos que $n = 7^{11}$ y $k = 3$ son primos relativos:

$$mcd(7,3) = 1$$
$$mcd(7^{11},3) = 1$$

Por tanto, hemos demostrado que podemos aplicar el teorema de Euler sobre $n =$ y $k = 3$, por lo que:

$$3^{\phi(7^{11})} \equiv 1 \pmod{7^{11}}$$
$$7^{11}|(3^{\phi(7^{11})}-1)$$
$$7^{11}|(3^{6\cdot 7^{10}}-1)\ \square$$

Ejercicio 7

Tenemos una hoja de papel, y se nos permite cortarla en 7 trozos distintos. Podemos repetir este proceso tantas veces deseemos. Es decir, podemos cortar

Solución

Cada vez que cortamos un trozo de papel en 7 estamos añadiendo 6 al total de trozos. Por tanto, todos los posibles números de trozos que puedo conseguir son congruentes entre sí módulo 6. Por ejemplo:

$$\begin{aligned} 7 \equiv 1 &\pmod 6 \\ 13 \equiv 7 \equiv 1 &\pmod 6 \\ 19 \equiv 13 \equiv 715 \equiv 7 \equiv 1 &\pmod 6 \\ &\vdots \end{aligned}$$

Buscamos el residuo de 1997 (los trozos pedidos) módulo 6:

$$1997 \equiv 5 \pmod 6$$

Como el residuo es distinto a 1, eso quiere decir que es imposible conseguir 1997 trozos usando el método indicado. □

Ejercicio 8

Considere la siguiente ecuación:

$$113x = 1 - 11y.$$

Utilizando el algoritmo del Pulverizador, encuentre la pareja de valores x e y solución de la ecuación con la y positiva más pequeña posible. La variable x puede ser negativa. Tanto x como y deben ser enteros.

Solución

Podemos escribir $113x = 1 - 11y$ como $113x + 11y = 1$, dándonos así cuenta de que x e y son una combinación lineal de 1. Planteamos el Pulverizador con $a = 113$ y $b = 11$:

a	b	res	$= a - q \cdot b$
113	11	3	$= 113 - 10 \cdot 11$
11	3	2	$= 11 - 3 \cdot 3 = 11 - 3(113 - 10 \cdot 11) = -3 \cdot 113 + 31 \cdot 11$
3	2	1	$= 3 - 1 \cdot 2 = (113 - 10 \cdot 11) - (-3 \cdot 113 + 31 \cdot 11) = 4 \cdot 113 - 41 \cdot 11$

Por tanto, tenemos que $x = 4$ e $y = -41$. Como queremos que $y > 1$,

Ejercicio 9

Encuentre el inverso multiplicativo de 6 más pequeño en módulo 25.

Solución

Como el $mcd(6, 25) = 1$, sabemos que 6 y 25 son primos relativos, por lo que podemos aplicar el Teorema de Euler para hallar el inverso multiplicativo. En primer lugar calculamos la función indicatriz de Euler de 25:

$$\phi(25) = \phi(5^2) = 25\left(1 - \frac{1}{5}\right) = 20$$

Por tanto, como $6^{\phi(25)} \equiv 1 \pmod{25}$, sabemos que el inverso multiplicativo de 6 en módulo 25 es:

$$6^{\phi(25)-1} = 6^{19}$$

Para encontrar el inverso multiplicativo más pequeño, calculamos el residuo módulo 72 de 6^{19}. Descomponemos 6^{19} en potencias de 2 y operamos:

$$\begin{aligned} 6^{19} &= 6^{16} \cdot 6^2 \cdot 6 \\ 6^2 &= 36 \equiv 11 \pmod{25} \\ 6^4 = (6^2)^2 &\equiv 11^2 = 121 \equiv 21 \pmod{25} \\ 6^8 = (6^4)^2 &\equiv 21^2 = 441 \equiv 16 \pmod{25} \\ 6^{16} = (6^8)^2 &\equiv 16^2 = 256 \equiv 6 \pmod{25} \\ 6^{19} &\equiv 6 \cdot 11 \cdot 6 = 396 \equiv 21 \pmod{25} \end{aligned}$$

Por tanto, el inverso multiplicativo de 6 módulo 25 es 21.

Ejercicio 10

Encuentre el inverso multiplicativo de 13 más pequeño en módulo 56.

Solución

Como el $mcd(13, 56) = 1$, sabemos que 13 y 56 son primos relativos, por lo que podemos aplicar el Teorema de Euler para hallar el inversio multiplicativo. En primer lugar calculamos la función indicatriz de Euler de 56:

$$13^{\phi(56)-1} = 17^{23}$$

Para encontrar el inverso multiplicativo más pequeño, calculamos el residuo módulo 56 de 13^{35}. Descomponemos 13^{35} en potencias de 2 y operamos:

$$\begin{aligned}
13^{23} &= 13^{16} \cdot 13^{4} \cdot 13^{2} \cdot 13 \\
13^{2} &= 169 \equiv 1 \pmod{56} \\
13^{4} = (13^{2})^{2} &\equiv 1^{2} = 1 \pmod{56} \\
13^{8} = (13^{4})^{2} &\equiv 1^{2} = 1 \pmod{56} \\
13^{16} = (13^{8})^{2} &\equiv 1^{2} = 1 \pmod{56} \\
13^{23} &\equiv 1 \cdot 1 \cdot 1 \cdot 13 = 13 \pmod{56}
\end{aligned}$$

Por tanto, el inverso multiplicativo de 13 módulo 56 es el propio 13.

Ejercicio 11

Indique si la relación aCb, definida como "las personas a y b cumplen años el mismo día" es una relación de equivalencia, razonando por qué. En caso de que la respuesta a la pregunta anterior sea afirmativa, indique también el número de clases de equivalencia que posee dicha relación.

Solución

Es una relación de equivalencia, ya que cumple las propiedades:

- **Reflexiva:** a cumple años el mismo día que a.
- **Simétrica:** Si a cumple años el mismo día que b, entonces b cumple años el mismo día que a.
- **Transitiva:** Si a cumple años el mismo día que b, y b cumple años el mismo día que c, entonces a cumple años el mismo día que c.

La relación tiene 365 clases de equivalencia, una para cada día del año. O, si se quieren considerar los años bisiestos, 366 clases de equivalencia.