Teoria de Números

Residuos

Olimpiada de Matemáticas en Tamaulipas

1. Introducción

Hasta ahora, al trabajar con números enteros siempre nos hemos estado preguntando¿divide el número a al número b? Al mantenernos dentro de éste enfoque estamos ignorando información, a saber: ¿al realizar la división a entre b cuál es el residuo? Muchas veces, ésta información es la importante.

Ejemplo 1: Una compañía de televisión por cable ofrece canales numerados del 1 al 500. Un televidente (compulsivo) enciende su televisor y éste se encuentra en el canal 123 que no le gusta. A continuación, el televidente presiona el botón de cambio de canal (hacia arriba) 12,345 veces consecutivas. ¿En qué canal se detiene?

Solución: Hay 500 canales. Cada 500 veces que el televidente presiona el botón vuelve al canal en el que inció. Notemos que $12,345 = 20(500) + 345$. Dicho con palabras, hay 20 grupos de 500 y sobran 345. Después de los 20 grupos de 500 el televidente está en el mismo canal del que inició, el 123. Lo único que importa en realidad es el "sobrante"de 345 cambios de canal. Y como empezó en 123, tenemos que 123+345=468 y éste es el canal en el que se detiene.

Ejemplo 2: Hoy es sábado 14 de septiembre del 2013, ¿qué día de la semana será el 14 de septiembre de 3013? Recordemos que un año es bisiesto si es múltiplo de 4 pero no es bisiesto si es múltiplo de 100 sin ser múltiplo de 200 (por ejemplo, 2100 y 2500 no serán bisiestos pero 2200 y 2800 sí).

Solución: La pregunta que debemos responder es la siguiente: ¿cuántos días van a pasar desde hoy hasta el 14 de septiembre de 3013? Una vez sabiendo esto, observemos que cada siete días volvemos al mismo día de la semana. Así que, de la misma forma que en el ejemplo anterior, todos los paquetitos de 7 días que se puedan formar no interesan, lo importante será saber cuál es el sobrante.

Para realizar el cálculo empezamos suponiendo que no hay años bisiestos. Entonces habría 1000(365)=365,000 días hasta la fecha que queremos. Luego, agregamos un día

por cada año bisiesto. Si no fuera por las reglas extra, habría un año bisiesto cada cuatro años. Eso es, 250 años bisiestos en un periodo de 1,000 años. Llevamos entonces 365,250 días. Sin embargo, las reglas extra nos dicen que 2100, 2300, 2500 y 2900 no serán bisiestos así que debemos quitar 4 días a nuestro cálculo. Por lo tanto, hemos visto que pasarán 365,246 días de aquí al 14 de septiembre de 3013. Realizando una división de casita vemos que $365,246 = (52,178)(7) + 0$. En otras palabras, 7 divide al total de días así que el 14 de septiembre de 3013 será sábado nuevamente!

A continuación, expresaremos las ideas que nos permitieron resolver los dos problemas anteriores de manera formal:

Teorema: Dados enteros a y b existen enteros q y r con $r < a$ tales que $b = q(a)+r$.

Nota para el entrenador: Aquí hay que recalcarle a los alumnos que el teorema anterior es simplemente la división de casita siendo b el número de adentro, a el de afuera, q el de arriba y r el de hasta abajo. Recordar que la maestra de primaria siempre nos decía que para que la división fuera correcta el número de abajo debía ser menor que el de afuera.

Al entero r se le llama el residuo de b módulo a

Definición: Si dos números b y c tienen el mismo residuo al dividirlos por un número a se dice que son *congruentes* y se escribe $b \equiv c \pmod{a}$.

Ejercicio: Determina si las siguientes afirmaciones son verdaderas o falsas:
$17 \equiv 9 \pmod{8}$, $253 \equiv 2 \pmod{5}$, $176 \equiv 193 \pmod{17}$.

Solución: Verdadera. Falsa. Verdadera.

La notación anterior puede parecer algo compleja y artificial, sin embargo es muy útil cuando se trabaja con problemas en que, como en los primeros ejemplos, solo nos interesa calcular un "sobrante". Esto se debe a que las congruencias pueden trabajarse (casi) como si fueran igualdades ya que cumplen las siguientes propiedades:

Propiedad 1: Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces $a + c \equiv b + d \pmod{m}$ y $a - c \equiv b - d \pmod{m}$. Es decir, podemos sumar o restar congruencias.

Nota para el entrenador: El hecho de que se puedan restar congruencias puede hacer que los alumnos tengan la duda de qué pasa si una de estas restas da un número negativo. Conviene aquí explicar que, en efecto, se pueden tener congruencias negativas y si se quiere se le puede sumar algo a ambos lados (usando la propiedad uno) para que queden números positivos.

Propiedad 2: Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces $ac \equiv bd \pmod{m}$. Es decir, podemos multiplicar las congruencias.

Nota para el entrenador: Recalcarle a los alumnos que se debe usar el *mismo* módulo siempre. Si no se usa el mismo módulo las propiedades *no* se pueden aplicar.

Ejemplo: Resolveremos el segundo ejemplo usando la notación desarrollada anteriormente y las propiedades 1 y 2. Ya vimos que el problema se reduce a responder la pregunta $365,246 \equiv ?\pmod 7$. Pero pudimos ahorranos tiempo viendo las congruencias módulo 7 de cada parte que fuimos calculando: $365 \equiv 1 \pmod 7$, $1000 \equiv 6 \pmod 7$ $250 \equiv 5 \pmod 7$ y $4 \equiv 4 \pmod 7$. Usando ahora las propiedades 1 y 2 concluímos que $365,246 \equiv 1000(365) + 250 - 4 \equiv 6(1) + 5 - 4 \equiv 7 \equiv 0 \pmod 7$, como habíamos calculado antes.

Ejercicio (para hacer en casa): Pedirle a los alumnos que calculen usando congruencias que día de la semana era el día que nacieron. (Luego pueden preguntarle a sus padres si la respuesta obtenida es correcta.)

Ejemplo: ¿Cuál es la última cifra de 3^{2013}?

Solución: Este problema puede solucionarse simplemente buscando un patrón: observemos que $3^1 = 3, 3^2 = 9, 3^3 = 27, 3^4 = 81$. Luego, como la última cifra de la siguiente potencia sólo depende de la última cifra de la anterior el patrón 3, 9, 7, 1, 3, 9, 7, 1 se irá repitiendo. Luego, como 2013= 503(4)+1 obtenemos que este ciclo de 4 se va a repetir 503 veces y nos sobra una. De manera que 3^{2013} tiene cifra final 3.

Sin embargo, éste problema también puede resolverse usando congruencias. Notemos, para empezar, que el problema en sí es una pregunta de congruencias: lo que queremos responder es $3^{2013} \equiv ?\pmod{10}$. (Porque al dividir cualquier número entre 10 el residuo que obtenemos es justamente la última cifra del número.) Luego vamos viendo que $3^1 \equiv 3 \pmod{10}$, $3^2 \equiv 9 \pmod{10}$, $3^3 \equiv 3^2(3) \equiv 9(3) \equiv 27 \equiv 7 \pmod{10}$, $3^4 \equiv 3^3(3) \equiv 7(3) \equiv 21 \equiv 1 \pmod{10}$. Pero entonces: $3^{2013} \equiv 3^{2012}(3) \equiv (3^4)^{503}(3) \equiv (1)^{503}(3) \equiv (1)(3) \equiv 3 \pmod{10}$. Que es lo que queríamos obtener.

Ambos procedimientos son equivlaentes, la diferencia es que el segundo está escrito en el lenguaje de congruencias. Una vez acostumbrados a utilizar la simbología de las congruencias estas nos permiten resolver muchos problemas. Notemos que las congruencias funcionan "casi"como igualdades porque, aunque podemos sumar restar y multiplicar, *no* podemos dividir cuando estamos usando congruencias. Igualdades como $2a \equiv b \pmod m \Rightarrow a \equiv \frac{b}{2} \pmod m$ pueden no tener sentido y no deben usarse. En el próximo entrenamiento de teoría de números desarrollaremos un procedimiento que nos permitirá, en algunos casos, "dividir". Por lo pronto, presentamos la más importante de las propiedades de las congruencias:

Propiedad 3: $a \mid b$ si, y sólo si, $b \equiv 0 \pmod a$.

Demostración: $b \equiv 0 \pmod a$ quiere decir que al dividir b entre a el residuo es 0. O en otras palabras, que podemos expresar b como $b = q(a) + 0$ para algún entero

q. Pero esto es lo mismo que decir que existe un entero q tal que $b = aq$ y esta es justamente la definición original que dimos de $a \mid b$. Por lo tanto, ambas afirmaciones son equivalentes.

En la practica, la propiedad 3 nos dice que las congruencias pueden utilizarse como una herramienta para demostrar divisibilidad.

Ejemplo: Demuestra que $5 \mid 7^{44} + 4^{77}$.

Demostración: Observemos que $7^1 \equiv 2 \pmod 5$, $7^2 \equiv 2(7) \equiv 14 \equiv 4 \pmod 5$, $7^3 \equiv 4(7) \equiv 3 \pmod 5$, $7^4 \equiv 3(7) \equiv 1 \pmod 5$. Luego, $7^{44} \equiv (7^4)^{11} \equiv (1)^{11} \equiv 1 \pmod 5$. Por otro lado, $4^1 \equiv 4 \pmod 5$, $4^2 \equiv 16 \equiv 1 \pmod 5$. Entonces, $4^{77} \equiv 4^{76}(4) \equiv 1(4) \equiv 4 \pmod 5$. Por lo tanto, $7^{44} + 4^{77} \equiv 1 + 4 \equiv 5 \equiv 0 \pmod 5 \Rightarrow 5 \mid 7^{44} + 4^{77}$.

2. Problemas

1. ¿Cuál es el año más cercano en el que el 14 de septiembre volverá a ser sábado?
2. Demuestra que $13 \mid 2^{2013} + 3^{2013} + 7$
3. Demuestra que $7 \mid 2222^{5555} + 5555^{2222}$
4. ¿Cuál es la última cifra de 7^{7^7}?
5. Demuestra que $2001 \mid 3(720^n - 30^n - 24^n + 1)$ para cualquier entero n.
6. Recordemos que un número n cuyas cifras son $a_m a_{m-1} \ldots a_1 a_0$ puede expresarse mediante su expansión decimal como $n = 10^m a_m + 10^{m-1} a_{m-1} + \ldots + 10a_1 + a_0$. Utiliza la expansión decimal y congruencias para explicar por qué funcionan los criterios de divisibilidad del 4, 8, 9 y 11
7. Si m es un entero cuya última cifra es 5, demuestra que:

$$1991 \mid 12^m + 9^m + 8^m + 6^m$$

8. El estudiante habrá observado que el objetivo en muchos de los problemas de éste entrenamiento era encontrar una potencia de un número que resultara congruente a 1 en el módulo que estábamos trabajando. El gran matemático francés Pierre Fermat proveyó un teorema que nos ayuda a encontrar ésto en varias situaciones:

   Teorema de Fermat: Sea p un número primo y a un entero tal que $p \nmid a$. Entonces $a^{p-1} \equiv 1 \pmod p$

Observa las tablas obtenidas en las soluciones de los problemas 2, 3 y 7. Utiliza el teorema de Fermat para resolver el siguiente problema:

Encuentra todos los primos p tales que $8p^4 - 3003$ también es primo.

3. Soluciones

1. Recordemos que $365 \equiv 1 \pmod 7$. Así que cada año que pasa le debemos sumar uno al día de la semana. Sin embargo, los años bisiestos tienen 366 días así que en éstos años debemos sumar dos. Debemos encontrar la primera ocasión en que hemos logrado sumar 7 o u otro múltiplo de 7. Entonces vemos la siguiente tablita:

Año	2014	2015	2016	2017	2018	2019
Suma acumulada	1	2	4	5	6	**7**

   Por lo tanto, el 2019 es el año buscado.

2. Para resolver el problema, realizamos la siguiente tabla:

n	1	2	3	4	5	6	7	8	9	10	11	12
$2^n \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1
$3^n \pmod{13}$	3	9	1	3	9	1	3	9	1	3	9	1

   Ahora observemos que $2013 = (167)(12)+9$. Esto nos dice que $2^{2013}+3^{2013}+7 \equiv 2^{2004}(2^9)+3^{2004}(3^9)+7 \equiv (2^{12})^{167}(2^9)+(3^{12})^{167}+7 \equiv (1)^{167}(5)+(1)^{167}(1)+7 \equiv 5+1+7 \equiv 13 \equiv 0 \pmod{13}$. Por lo tanto, $13 \mid 2^{2013}+3^{2013}+7$.

3. Observemos que $2222 \equiv 3 \pmod 7$ y $5555 \equiv 4 \pmod 7$. Por lo tanto, usando la propiedad 2, $2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod 7$.

   Nota para el entrenador: Recalcarle a los alumnos que no es correcto a partir de $2222 \equiv 3$ (mod 7) y $5555 \equiv 4$ (mod 7) concluir que $2222^{5555} + 5555^{2222} \equiv 3^4 + 4^3$ (mod 7)

   Ahora, realizamos la siguientes tablitas:

n	1	2	3	4	5	6
$3^n \pmod 7$	3	2	6	4	5	1

   Luego, $5555 = 925(6)+5$ y $2222 = 740(3)+2$ así que $3^{5555}+4^{2222} \equiv (3^6)^{925}(3^5)+(4^3)^{740}(4^2) \equiv (1)(5)+(1)(2) \equiv 7 \equiv 0 \pmod 7$. Por lo tanto, $7 \mid 2222^{5555} + 5555^{2222}$.

n	1	2	3
$4^n \pmod 7$	4	2	1

4. Nuevamente, la pregunta que debemos responder es: $7^{7^7} \equiv ? \pmod{10}$. Empecemos viendo que $7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$, $7^4 \equiv 1 \pmod{10}$. De tal manera que la última cifra se irá repitiendo en un ciclo de 4 elementos $7 \to 9 \to 3 \to 1 \to 7 \ldots$

   Ahora bien, ¿qué información necesitamos para saber cuál es la última cifra de 7^n para cualquier entero n? Solamente necesitamos saber el residuo de dividir n entre 4. En otras palabras, si sabemos que $n = 4q + r$ con $r < 4$ entonces tenemos que $7^m \equiv (7^4)^q(7^r) \equiv (1)(7^r) \pmod{10}$. Así que nuestra pregunta se redujo a responder la pregunta $7^7 \equiv ? \pmod 4$.

   Vemos que $7^1 \equiv 3 \pmod 4$, $7^2 \equiv 1 \pmod 4$, por lo tanto $7^7 \equiv (7^2)^3(7) \equiv (1)(3) \equiv 3 \pmod 4$. Entonces la última cifra de 7^{7^7} es 3.

5. Podríamos pensar en aplicar directamente congruencias módulo 2001 pero esto sería demasiado trabajoso. En lugar de esto, empecemos factorizando 2001: $2001 = 3 \times 23 \times 29$. Por lo que hemos visto en entrenamientos anteriores, para ver que 2001 divide a algo, podemos en su lugar ver que 3 lo divide que 23 lo divide y que 29 lo divide. Observemos que automáticamente 3 divide a $3(720^n - 30^n - 24^n + 1)$ así que sólo nos falta ver que 23 y 29 dividen a $(720^n - 30^n - 24^n + 1)$.

   Empecemos trabajando con el módulo 23: $720 \equiv 7 \pmod{23}$, $30 \equiv 7 \pmod{23}$ y $24 \equiv 1 \pmod{23}$. Por lo tanto, $720^n - 30^n - 24^n + 1 \equiv 7^n - 7^n - 1^n + 1 \equiv 0 \pmod{23}$ sin importar cuanto valga n. Por lo tanto, $23 \mid 720^n - 30^n - 24^n + 1$ para cualquier n entero.

   De la misma manera, para el módulo 29: $720^n \equiv 24 \pmod{29}$ y $30 \equiv 1 \pmod{29}$ así que $720^n - 30^n - 24^n + 1 \equiv 24^n - 1^n - 24^n + 1 \equiv 0 \pmod{29}$ sin importar cuanto valga n. Entonces, hemos demostrado que $29 \mid 720^n - 30^n - 24^n + 1$ para cualquier n. Pero esto nos basta para concluir lo que queremos.

6. Empecemos por el criterio del 4. Tenemos el número $n = 10^m a_m + 10^{m-1}a_{m-1} + \ldots + 10a_1 + a_0$. Queremos demostrar que $4 \mid n$ si y sólo si $4 \mid 10a_1 + a_0$ (el número formado por las últimas dos cifras). Observemos que si $k \geq 2$ entonces $4 \mid 10^k$, o equivalentemente, $10^k \equiv 0 \pmod 4$. Por lo tanto, $10^m a_m + 10^{m-1}a_{m-1} + \ldots + 10a_1 + a_0 \equiv (0)a_m + (0)a_{m-1} + \ldots + (0)a_2 + 10a_1 + a_0 \equiv 10a_1 + a_0 \pmod 4$. Es por esto que para ver si $4 \mid n$ basta fijarse en las últimas dos cifras.

   De la misma manera podemos verificar el criterio del 8. Ahora tenemos que si $k \geq 3$ entonces $8 \mid 10^k$. Por lo tanto, $n \equiv 10^m a_m + 10^{m-1}a_{m-1} + \ldots + 10a_1 + a_0 \equiv$

$10^2a_2+10a_1+a_0 \pmod 8$. Pero $10^2a_2+10a_1+a_0$ es justamente el número formado por las últimas 3 cifras.

Ahora, para el criterio del 9 vemos que $10 \equiv 1 \pmod 9 \Rightarrow 10^k \equiv 1 \pmod 9$ para cualquier k. Por lo tanto, $n \equiv 10^m a_m + 10^{m-1}a_{m-1} + \ldots + 10a_1 + a_0 \equiv a_m + a_{m-1} + \ldots + a_1 + a_0 \pmod 9$. Pero ésto último es precisamente la suma de las cifras. Así que hemos visto que n tiene la misma congruencia módulo 9 que la suma de sus cifras (en particular n es divisible por 9 si dicha congruencia es 0 pero entonces la suma de sus cifras también tiene congruencia 0 y también es divisible y éste es el criterio del 9.)

Finalmente, para el caso del 11 vemos que $10 \equiv -1 \pmod{11}$ implica que $10^k \equiv 1 \pmod{11}$ si k es par y $10^k \equiv -1 \pmod{11}$ si k es impar. Por lo tanto, n será congruente a la suma de las cifras pares menos las suma de las cifras impares. Pero este es justamente el criterio del 11.

7. Nuevamente, es conveniente empezar por factorizar 1991: Vemos que $1991 = 11 \times 181$. La diferencia con el problema anterior es que ahora también podemos factorizar la otra expresión (hemos visto en entrenamientos anteriores que cuando tenemos sumas algebraicas es conveniente factorizarlas para convertirlas en productos): $12^m+9^m+8^m+6^m = (3^m)(4^m)+(3^m)(3^m)+(2^m)(4^m)+(2^m)(3^m) = (3^m)(4^m+3^m)+(2^m)(4^m+3^m) = (3^m+2^m)(4^m+3^m)$. Por lo tanto, lo que queremos demostrar es que 11 y 181 dividen a $(2^m+3^m)(3^m+4^m)$ cuando m con útima cifra 5.

Empecemos con el módulo 11. Realizamos las tablitas usuales:

m	1	2	3	4	5	6	7	8	9	10
$2^m \pmod{11}$	2	4	8	5	10	9	7	3	6	1

n	1	2	3	4	5
$3^n \pmod{11}$	3	9	5	4	1

n	1	2	3	4	5
$4^n \pmod{11}$	4	5	9	3	1

Ahora, un entero m que tiene última cifra 5 podemos escribirlo como $m = 10q+5$ para algún entero q. Entonces, $2^m \equiv (2^{10})^q(2^5) \equiv (1)(5) \equiv 5 \pmod{11}$. Mientras que, $3^m \equiv (3^5)^{2q+1} \equiv 1^{2q+1} \equiv 1 \pmod{11}$ y de la misma manera podemos ver que $4^m \equiv 1 \pmod{11}$. Podemos ver entonces que $2^m + 3^m \equiv 1 + 10 \equiv 11 \equiv 0 \pmod{11}$. Por lo tanto, $11 \mid 2^m + 3^m$ y evidentemente $11 \mid (2^m + 3^m)(3^m + 4^m)$.

Entonces, para terminar nos enfocaremos en ver que $181 \mid 3^m + 4^m$. Hacemos las tablitas módulo 181:

n	1	2	3	4	5	6	7	8	9	10
$3^n \pmod{181}$	3	9	27	81	62	5	15	45	135	43
$4^n \pmod{181}$	4	16	64	75	119	114	94	14	56	43

Ahora, nuevamente utlilizando que m lo podemos escribir como $m = 10q + 5$, vemos que $3^m + 4^m \equiv 3^{10q+5} + 4^{10q+5} \equiv (3^{10})^q(3^5) + (4^{10})^q(4^5) \equiv (43^q)(62) + (43^q)(119) \equiv (43^q)(62 + 119) \equiv (43^q)(181) \equiv 0 \pmod{181}$. Por lo tanto, $181 \mid 3^m + 4^m$ y esto nos basta para terminar.

8. Si p es un primo distinto de 5, entonces $5 \nmid p$. Luego, por teorema de Fermat, $p^4 \equiv 1 \pmod 5$. Luego, $8 \equiv 3 \pmod 5$ y $3003 \equiv 3 \pmod 5$ nos dicen que $8p^4 - 3003 \equiv 3(1) - 3 \equiv 0 \pmod 5$. Es decir, hemos demostrado que si $p \neq 5$ entonces $5 \mid 8p^4 - 3003$. Queremos que esta expresión sea un primo pero el único primo divisible por 5 es el 5 mismo. Verifiquemos si ésto es posible: $8p^4 - 3003 = 5 \Rightarrow 8p^4 = 3008 \Rightarrow p^4 = 376$ pero no hay primo que cumpla esta igualdad.

   La única opción que nos queda es $p = 5$. Veamos si cumple: $8(5)^4 - 3003 = 8(625) - 3003 = 5000 - 3003 = 1997$ y podemos verificar que en efecto es primo. Asi que la única solución es $p = 5$.