Módulos y Teoremas de Divisibilidad

Entrenamiento #5 para 3ª etapa
09-15 de abril de 2016
Por: Lulú

Resumen

Bienvenidos sean de nuevo a Números. Como el título del documento lo dice, ahora habremos de hablar sobre los módulos y los diferentes teoremas de divisibilidad que ello conlleva. También revelaremos cómo es que ya lo hemos trabajado sin saber.

1. Un pequeño preámbulo

¿Recuerdas en la sesión pasada de Teoría de Números, cuando decíamos que una pareja de enteros a y b podían escribirse de la manera $a = mp + r_1$ y $b = mq + r_2$? ¿Y te acuerdas también que si $m|a$, entonces $r_1 = 0$? En caso de que no, eso es fácil de ver. Bueno, espero que al menos recuerdes que hacer operaciones entre números equivalía, en cierta manera, a hacer operaciones con los residuos. Siendo así, ¿cuándo sabemos que $m|a - b$?

Para refrescar un poco la memoria, hagamos juntos aquí dicha resta. Recordemos también que $0 \leq r < m$. Entonces, $a - b = (mp + r_1) - (mq + r_2) = mp + r_1 - mq - r_2 = m(p - q) + (r_1 - r_2)$. Sabemos que $m(p - q)$ es claramente divisible entre m, pero ¿cómo aseguramos que $r_1 - r_2$ es divisible entre m si cada una de ellas (las r's) es menor que m y, además, se están restando? ¿Qué múltiplo de m es mayor que $-m$ y menor a m? El cero; $r_1 - r_2$ debe ser igual a 0. Puedes pensar en cualquier ejemplo si lo necesitas. Date tiempo para comprender y asimilar estas cosas.

Aquí empezaremos a definir los módulos. $a \equiv b \pmod{m}$, que se lee como "a es congruente con b módulo m", y significa que $m|a - b$ ó (lo que es lo mismo) $\frac{a-b}{m} \in \mathbb{Z}$. Con base en lo que hemos explicado antes, eso también puede interpretarse de otra manera: ¡que a y b tienen el mismo residuo! Claro que, debe decirse, al ser divididos entre m. Por eso se hace la referencia y se dice "módulo m". También es de aquí obvio que todo número es congruente con su residuo módulo m.

Por cierto, advierto que esta lista de problemas es larga. Espero que la encuentren de provecho y se diviertan en el proceso.

2. Módulos y operaciones modulares

Imaginemos que estamos lunes 3 de algún mes. Si te preguntan "¿qué día es dentro de 18 días?", ¿cómo le harías?. Quizá yo soy el único raro que lo hace de esa manera, pero normalmente pienso "oh, 18 días son dos semanas y 4 días. Por lo tanto, sólo tengo que sumarle 4 días a lunes y eso es un viernes". Si tú en algún momento pensaste así o hiciste algo parecido: ¡felicidades, ya has utilizado la lógica de módulos y residuos! Pero, por favor, no le digas al resto de tus amigos que así haces las cosas. Sé lo que te digo.

Entonces, como te habrás dado cuenta, cuando usas un módulo m el residuo se mantiene cada m enteros. En el ejemplo pasado el módulo era 7 y sabemos que después de 7 días estamos en lunes otra vez. O si lo vemos con los meses, cada 12 meses. Módulos *are everywhere*.

Veamos otro ejemplo con días de la semana. Supongamos que hoy es viernes: ¿qué día será cuando hayan pasado exactamente 500 días? Si vemos que cada 7 días es viernes de nuevo, entonces sólo hay que ver cuántos días

sobran. Es decir cuántos días quedan que no se pudieron encasillar a una semana completa. Como el residuo de dividir 500 entre 7 es 3, entonces sólo hay que sumar 3 días y eso sería un lunes.

Y bueno, así como les comenté en la sesión anterior de Teoría de Números y al principio de este documento, las operaciones con números también se pueden hacer con sus residuos (no todas).

2.1. Operaciones con residuos

Primero que nada, hay que decir que las congruencias son transitivas en cierta manera. ¿A qué me refiero? Pensemos en un número $a = mq_1 + r$ que sea congruente con $b = mq_2 + r$ y un c que sea congruente con b (obviamente todos son bajo módulo m). Pero, el hecho de que $b \equiv c$ significa que el residuo de c y el de b son iguales; de modo que $c = mq_3 + r$. Pero r es el mismo residuo de a, por lo que $a \equiv b \equiv c \pmod{m}$. Además, es claro que todo número es congruente consigo mismo.

Eso es como un pequeño preámbulo para empezar a las operaciones que son legales bajo el marco de las congruencias. Se muestran a continuación:

1. Suma de congruencias
2. Producto de congruencias
3. Potencias de congruencias
4. El fantabuloso y particular caso de la división de congruencias

2.1.1. Suma de congruencias

Si $a \equiv b \pmod{m}$ podemos decir que $a = mq_1 + r_1$ y que $b = mq_2 + r_1$ ya que al ser congruentes tienen necesariamente el mismo residuo. Por otro lado, supongamos que $c \equiv d \pmod{m}$, con $c = mq_3 + r_2$ y $d = mq_4 + r_2$.Si sumamos a con c y b con d, se tiene

$$a + c = m(q_1 + q_3) + (r_1 + r_2)$$
$$b + d = m(q_2 + q_4) + (r_1 + r_2)$$

Con ello es claro que $a + c \equiv b + d \pmod{m}$, pues ambos tienen el mismo residuo. Además, si se dice no sólo que $c \equiv d$ sino que $c = d$, se tendría $a + c \equiv b + c$. Hemos de recordar que también podemos utilizar números negativos, de modo que sumarlos sería como hacer una resta.

2.1.2. Producto de congruencias

De la misma forma, con los mismos a, b, c, d, si se multiplican a con c y b con d, se tiene que:

$$ac = m^2 q_1 q_3 + mq_1 r_2 + mq_3 r_1 + r_1 r_2 = m(mq_1 q_3 + q_1 r_2 + q_3 r_1) + (r_1 r_2)$$
$$bd = m^2 q_2 q_4 + mq_2 r_2 + mq_4 r_1 + r_1 r_2 = m(mq_2 q_4 + q_2 r_2 + q_4 r_1) + (r_1 r_2)$$

De aquí, como todo está expresado de la forma $mq + r$, es claro que $ac \equiv bd \pmod{m}$. Y claro que si $c = d$, sería como multiplicar ambos lados por una misma constante. Y, sí, también se puede con número negativos.

2.1.3. Potencias de congruencias

Aquí bastará con $a = mq_1 + r_1$ y $b = mq_2 + r_1$. Si se eleva (o se multiplica por sí mismo) cada uno de ellos un total de k veces habrá, en cada caso, sólo un término en el que no aparezca la m, y ese será r_1^k. Si no me crees puedes verificarlo con el binomio de Newton. El punto es que para ambos se tendrá un residuo de r_1^k; por lo que, al tener el mismo residuo, son congruentes. Si no te queda muy claro, puedes hacer las cuentitas o pedirle amablemente (y con galletas) a tu entrenador que lo haga en el pizarrón.

2.1.4. El fantabuloso y particular caso de la división de congruencias

No es que no puedan hacerse. Sí se puede dividir. Pero tiene sus restricciones. Pero sólo cuando el factor que se tiene que eliminar es primo relativo con el módulo. Es decir que si $ax \equiv bx \pmod{m}$, siendo x y m coprimos, entonces $a \equiv b \pmod{m}$.

Por ejemplo, si decimos $4k \equiv 24 \pmod{24}$ sería erróneo asegurar que $k \equiv 6 \pmod{24}$. Si $k \equiv 0, 12, 18$ también funciona. Por eso digo que no puedes asegurar nada.

2.2. Cómo utilizar las operaciones para hacer problemas

Un pequeño ejemplo de cómo usar las propiedades anteriores y, en conjunto con una sugerencia personal, sería un problema como el que nos pide encontrar todos los valores de n para los cuales $3|n^2+1$.

La sugerencia que yo les hago es una "tabla de residuos". Por un lado se dejan los posibles residuos, y por otro se van haciendo operaciones. Para el ejemplo dado sería algo así:

$n \pmod 3$	$n^2 \pmod 3$	$n^2+1 \pmod 3$
0	0	1
1	1	2
2	1	2

Primero, la tabla está construida de manera que la primera columna muestra todos los residuos módulo 3. Ésto es porque estamos revisando la divisibilidad entre 3, bajo pedido del problema. La segunda columna tiene el residuo de n^2 pero, como ya se ha dicho, en congruencias hacemos operaciones sólo con los residuos; de ese modo sólo basta con elevar los residuos al cuadrado. La tercera columna muestra los residuos módulo 3 de n^2+1. Para que eso fuera divisible entre 3, el residuo tendría que ser cero; pero como nunca el residuo es cero, entonces no hay ninguna n que cumpla.

En cambio si el problema fuera encontrar todos los enteros n tales que $4|3n^3+1$, la tabla cambiaría un poco.

n	n^2	n^3	$3n^3$	$3n^3+1$
0	0	0	0	1
1	1	1	3	0
2	0	0	0	1
3	1	3	1	2

Tabla de residuos con módulo 4

Para esta tabla vemos que hay un renglón que sí da un residuo cero: el renglón de los $n \equiv 1$. Entonces los n tales que $n \equiv 1 \pmod 4$ cumplen. Esto puede reinterpretarse como todos los números de la forma $4k+1$. Intentemos con el 1: $3 \times 1^3 + 1 = 3 \times 1 + 1 = 3 + 1 = 4$, que sí es divisible entre 4. Con $n = 5$, se tiene $3 \times 5^3 + 1 = 3 \times 125 + 1 = 375 + 1 = 376$, que también es divisible entre 4.

Espero que con estos ejemplos haya quedado un poquito más claro. Si no, pos ahí están los entrenadores para que preguntes.

2.3. Teoremas Wakala

No sé si se llamen así. Ni siquiera sé si tienen nombre. Pero hubo una vez en la que me sentí frustrado por querer referenciar estos teoremas y no poder hacerlo debido a la falta de nombre. ¿Cómo solucioné esa situación? Le di un nombre. Lamentablemente no soy lo suficientemente creativo y sólo se me ocurrió llamarlos "Teoremas

Wakala". Bueno, pero ya fue mucha historia. Probablemente quieras saber qué es, qué dice, para qué sirve, con qué se come.

Bueno, a resumidas cuentas, y enlistados, dicen que (considerando que a, b son dos enteros y que n es un número natural):

1. $a+b|a^n+b^n$ cuando n es impar.
2. $a+b|a^n+b^n$ cuando n es par.
3. $a-b|a^n-b^n$ para cualquier n.

Demostraré el tercero y tú harás los demás (por eso es uno de los problemas de la lista). Consideremos el hecho de que todo número es congruente a sí mismo y a su residuo. El residuo de $a-b$ módulo $a-b$ es claramente 0. Por lo tanto:

$$\begin{aligned} a-b &\equiv 0 \pmod{a-b} \\ a &\equiv b \pmod{a-b} \\ a^n &\equiv b^n \pmod{a-b} \\ a^n-b^n &\equiv 0 \pmod{a-b} \end{aligned}$$

Mira, aquí va despacito. Primero, todo número (en este caso $a-b$) es congruente a su residuo. Como queremos revisar la divisibilidad entre $a-b$ ese fue también el módulo. Y pues, el residuo de cualquier cosa entre sí misma es cero. Luego, por la propiedad de las sumas, es posible sumar b en ambos lados de la congruencia. Luego, por la propiedad de las potencias de congruencias, fue posible elevar legalmente a la n. Luego es sólo cuestión de "pasar restando" el $-b^n$. De modo que nos queda que a^n-b^n deja el mismo residuo (es congruente) que cero módulo $a-b$; pero el residuo de cero siempre es cero (cabe cero veces en la división y sobran cero). Por lo tanto, el residuo de a^n-b^n es cero, lo que significa que es divisible entre el módulo. Y hemos concluido.

Ahora sigue leyendo, que al rato te tocará hacer los demás.

2.4. Un pequeño repaso

¿Qué hemos aprendido hoy? Como toda la información está dispersa a lo largo del documento, creí que sería buena idea juntar todo aquí.

1. Todo número es congruente con su propio residuo módulo lo que sea
2. Todo número es congruente con sí mismo módulo lo que sea
3. Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$
4. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $a+c \equiv b+d \pmod{m}$
5. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $ac \equiv bd \pmod{m}$
6. Si $a \equiv b \pmod{m}$, entonces $a^k \equiv b^k \pmod{m}$, para cualquier k entera no negativa'
7. Si $ax \equiv bx \pmod{m}$ sucede que $a \equiv b \pmod{m}$ sólo si x y m son primos relativos
8. Los Teoremas Wakala

Listo. Ahora, ¿qué estás esperando? ¡A darle!

3. Ejercicios

1. Una rueda de la fortuna circular tiene 20 asientos numerados en orden del 1 al 20. Si el asiento que está a la altura del piso es el asiento 2, y la rueda de la fortuna se mueve 36 asientos, ¿cuál será el que esté a la altura del piso? (Por ejemplo, si se hubiera movido 3 asientos, entonces los asientos se mueven así: $3 \to 4 \to 5 \to 6$, y el que queda a la altura del piso es el asiento 6).

2. Un cronómetro marca desde el minuto 0 hasta el minuto 59. Cuando marca el minuto 59 y pasa otro minuto, el cronómetro marca de nuevo el minuto 0. Si en un determinado momento el cronómetro marca 13 minutos, y pasan exactamente 80 minutos, ¿qué minuto marcará el cronómetro? ¿Y si pasan 1201 minutos?

3. Si $k \equiv 1$ (mód 4), ¿a qué es congruente $6k + 5$ (mód 4)?

4. ¿Cuál es el residuo de $2010 \times 2011 \times 2012 + 2013^2$ cuando se divide entre 7?

5. ¿Cuál es el residuo cuando se divide 9^{2013} entre 8?

6. Sean $N = 22 \times 31 + 11 \times 17 + 13 \times 19$. Determina:

   a) la paridad de N

   b) el dígito de las unidades de N

   c) el residuo cuando N se divide entre 7

7. ¿Cuál es el último dígito de 7^{2015}?

8. ¿Cuál es el último dígito de 3^{1234}?

9. ¿Cuál es el dígito de las unidades de $1! + 2! + 3! + \cdots + 9! + 10!$?

10. Demuestra que $41 | 2^{20} - 1$.

11. ¿Puede $N = 222222$ ser un cuadrado perfecto?

12. ¿Puede ser $N = 2727272727$ un cuadrado perfecto?

4. Agregados culturales

1. En caso de que te hayas quedado con la duda, $\mathbb{Z}$ representa el conjunto de los enteros.

2. Decir que $x \in \mathbb{Z}$ se lee "x pertenece a los enteros", lo que significa que es un entero.

3. Por si también lo olvidaste $a|b$ se lee (y significa) "a divide a b".

4. Otras personas sí se han referido a los Teoremas Wakala en sus exámenes bajo ese nombre. Lamentablemente, debido a que no hay un nombre oficial para esos teoremas, esa práctica ha caído en desuso y es también poco recomendable.

5. La primera vaca en volar dentro de un avión fue, por extrañas razones del destino, también la misma en ser ordeñada en un avión. "Nellie Jay" (mejor conocida como "Elm Farm Ollie"), una vaca Guernsey de la granja Elm, hizo historia el 18 de febrero de 1930.

5. Lista de problemas

1. Encuentra los últimos dos dígitos de 3^{1234}
2. Encuentra el último dígito de 7^{7^7}.
3. Demuestra que $7|2222^{5555} + 5555^{2222}$.
4. Demuestra que $n^3 + 2n$ es divisible por 3 para cualquier número entero positivo n que se elija.
5. Demuestra que $n^5 + 4n$ es divisible por 5 para cualquier entero positivo n.
6. Demuestra que $a(a+1)(2a+1)$ es divisible por 6 para todo entero positivo a.
7. ¿Es cierto que si $a^2 \equiv b^2$ (mód n) entonces siempre se tiene que $a \equiv b$ (mód n)?
8. Encuentra todos los enteros m tales que $1066 \equiv 1776$ (mód m).
9. Demuestra los **Teoremas Wakala**.
10. Demuestra los criterios de divisibilidad de los números del 2 al 11, sin incluir el 7.
11. Encuentra todos los enteros positivos n tales que $9|n^3 + 2$.
12. Demuestra que la diferencia de dos cubos perfectos consecutivos no puede ser múltiplo de 3.
13. Demuestra que para toda n entera sucede que
$$3804|(n^3 - n)(5^{8n+4} + 3^{4n+2})$$
14. Prueba que:
    a) Todo primo mayor a 2 es congruente a 1 ó 3 módulo 4.
    b) Todo primo mayor a 3 es congruente a 1 ó 5 módulo 6.
15. Si p es un primo mayor 3, prueba que $24|p^2 - 1$.
16. Sean x, y dos números enteros. Demuestra que si $3|x^2 + y^2$, entonces $3|x$ y $3|y$.
17. Prueba que si $27|\overline{abc}$, entonces $27|\overline{cab}$.
18. Demuestra que si $n \equiv 4$ (mód 9), entonces n no puede escribirse como la suma de tres cubos.
19. Sean x, y, z tres números enteros. Demuestra que si $7|x^3 + y^3 + z^3$, entonces 7 divide a alguno de los tres enteros.
20. Sean a, b, c tres números enteros. Demuestra que si $9|a^3 + b^3 + c^3$, entonces $3|abc$.
21. Demuestra que
$$2013|1^{2013} + 2^{2013} + 3^{2013} + \cdots + 2011^{2013} + 2012^{2013} + 2013^{2013}$$
22. Encuentra todas las parejas de enteros positivos impares (a, b) tales que $a^2 + b^2$ sea un cuadrado perfecto.
23. Sea a, b, c dígitos que cumplen las siguientes condiciones:
    a) $3|\overline{abc} + a$
    b) $2|\overline{cba}$
    c) $5|\overleftarrow{bac}$

Demuestra que:

$$2010|(94a^2c + 47abc + 47ac^2)^{2011} + (40a^2c + 20abc + 20ac^2)^{2011}$$

24. Demuestra que no existen enteros a, b, c tales que $a^2 + b^2 = 8c + 6$.

25. Encuentra todas las parejas de enteros positivos (a, b) tales que $a^4 + 1$ y $b^2 + 1$ no son divisibles por 39 pero $(a^4 + 1)(b^2 + 1)$ sí lo es.

26. Determina el máximo común divisor de todos los números de la forma $16^n + 10n - 1$, donde n es un entero positivo.

27. ¿Puede ser un número $A = 11...1$ (consistente de 300 unos) ser un cuadrado perfecto?

28. En un tablero de 1×2012 se encuentran escritos los números del 1 al 2012, no necesariamente en orden. Dos jugadores A y B juegan por turnos, cada uno haciendo una jugada por turno. El jugador A comienza. Una jugada consiste en tomar una casilla y pintarla de rojo o azul. Una casilla pintada no puede volver a ser coloreada. Cuando se pinta todo el tablero, se toman las casillas coloreadas con azul y se suman los números en ellos. Si el número resultante es divisible entre 3, gana B. De lo contrario, gana A.

29. ¿Cuál es la última cifra distinta de cero de 100!?

30. ¿Cuál es el dígito de las unidades de

$$\sum_{k=1}^{2009} (k^2 + k)?$$

31. ¿Cuántas parejas de números (a, b) hay tales que a y b son enteros en el rango de 1 a 100?

32. Sean n, m, r tres números naturales que $n^2 + m^2 = r^2$ (forman una terna pitagórica). Prueba que $30|nmr$.

33. ¿Cuál es el criterio de divisibilidad de 2^n? Demuéstralo.

6. Problemas más jarcors

1. Demuestra los criterios de divisibilidad del 7 y el 13.

2. Si n es un entero positivo mayor que 1 tal que $2^n + n^2$ es un número primo, demuestra que $n \equiv 3$ (mód 6).

3. Demostrar que para todo $n \in \mathbb{N}$:

   a) $7|3^{2n+1} + 2^{n+2}$
   b) $11|3^{2n+2} + 2^{6n+1}$

4. Encuentra todas las cuartetas de primos (p, q, r, s) tales que $p < q < r < s$ y además

$$p^2 + q^2 + r^2 + s^2 = 2013$$

5. ¿Cuál es el máximo común divisor de los números $p^4 - 1$, donde p es un primo mayor que 5?

6. Sean $1 = d_1 < d_2 < d_3 < ... < d_k = n$ los divisores positivos del entero positivo n. Encuentra todos los números n tales que $n = d_2^2 + d_3^3$.

7. Encuentra todos los números de 7 dígitos que son múltiplos de 3 y de 7, y cada uno de cuyos dígitos es 3 ó 7.

8. Encuentra el menor entero positivo tal que al escribirlo en notación decimal utiliza exactamente dos dígitos distintos y que es divisible entre cada uno de los números del 1 al 9.