Repaso de divisibilidad y leve introducción a residuos

Teoría

Hemos visto ya pues varias cosas interesantes de Teoría de número que nos permiten englobar distintos temas e incluso usarlos juntos.

Paridad

Una propiedad interesante a analizar de los números enteros es su paridad y cómo se modifica esta al realizar operaciones con los números. Recordando pues, la suma de dos números con la misma paridad, nos dará siempre un número par y la suma de dos números de distinta paridad nos dará siempre un número impar. Así pues, la resta será también equivalente a la operación de la suma.

Destaca aparte, el hecho de que al multiplicar un número par por cualquier número entero, este seguirá siendo par. De este hecho, proviene que un número impar nunca podrá ser divisible entre un número par, truco que puede aparece a veces para descartar casos en algunos problemas.

Criterios de divisibilidad

Tenemos algunas formas rápidas de corroborar si un número es múltiplo de algunos números en particular:

Número	**Criterio**
2	Su última cifra es par (0, 2, 4, 6 u 8)
3	La suma de sus cifras es múltiplo de 3
4	Sus últimas dos cifras forman n número múltiplo de 4
5	Su última cifra es 0 o 5
6	Cumple los criterios del 2 y el 3
7	Se toma la última cifra del número y su doble se le resta al número formado por las cifras restantes, si ese número es múltiplo de 7, el número original lo es
8	Sus últimas tres cifras forman un número múltiplo de 8
9	La suma de sus cifras es múltiplo de 9
10	Su última cifra es 0
11	Si a la suma de las cifras en posición par le restamos la suma de la cifra en posición impar, y ese número es múltiplo de 11, entonces el número original lo es
General	Hacer la división y comprobar que el residuo da cero

Números primos

Los números primos son números que sólo son divisibles entre los divisores triviales, es decir, entre 1 y el mismo número. Cabe recalcar que el 1 no es primo y se le conoce como unidad, y los números que no son primos ni la unidad, se llaman compuestos. Los números primos entonces son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, …

Para saber si un número es primo, se puede realizar de dos formas:

1) **Criba de Eratóstenes:** La criba de Eratóstenes consiste en una tabla en la cual están escritos los números del 1 hasta el número que deseemos saber. Al principio se tacha el número 1, pues este no es primo. En cada paso, se buscará el primer número que no esté tachado y que no hayamos reconocido como primo y entonces ese número será primo. Posteriormente, tachamos todos sus múltiplos; repetimos este proceso sucesivamente hasta que no haya más números que tachar (esto pasará cuando el número primo que identifiquemos sea mayor a la raíz del tamaño de la tabla, los números que queden sin tachar, serán en automático números primos). Conviene hacer la tabla con 6 columnas pues esto facilita tachar los múltiplos de 2, 3, 5 y 7.
2) **Prueba hasta la raíz:** La segunda forma de hacerlo es probando con los números más chicos a ver si alguno divide al número que queremos ver si es primo. La observación interesante es que sólo debemos probar con los números primos hasta la raíz del número que estamos analizando, puesto que todo número compuesto debe tener un divisor primo menor a su raíz.

Teorema fundamental de la aritmética

Aquí cobra importancia la definición de los números primos, ya que debido a su naturalez de ser "indivisibles", se cumplirá uno de los teoremas más importantes en la teoría de números, el Teorema fundamental de la aritmética, que dice así:

Todo número entero positivo mayor o igual a 1, se puede factorizar en números primos de una y sólo una manera salvo el orden.

Esto tiene implicaciones importantes, pues entonces, todos los números podrán ser factorizados de una única forma en números primos, y además, esto nos permite "analizar" o "conocer" muchas propiedades de los números sólo viendo su factorización.

Algunas de las principales características que podemos analizar son:

Ceros al final de un número	Basta con analizar el número de factores 5 y factores 2 que tiene el número, ya que un cero se agregará al final del número cuando haya un 10 (una pareja de 2x5)
Divisores y múltiplos de un número	Para que un número x divida a y, es necesario que la factorización en primos de x no contenga ningún primo que no esté en la factorización de y, y además que los exponentes de cada primo en la factorización de x sean menores o iguales al exponente en la factorización de y
Número de divisores de un número según su factorización	Al tener la factorización en primos de un número, por ejemplo del $72 = 2^3 3^2$, observamos que por la propiedad anterior, los divisores del número sólo podrán ser números de la forma $2^a\,3^b$ donde $0 \leq a \leq 3$ y $0 \leq b \leq 2$ por lo cual en total habrá 4×3 posibles combinaciones de los factores.

Factorización de potencias perfectas	Es fácil demostrar que por las propiedades de los exponentes, la factorización del cuadrado de un entero siempre deberá de tener sólo exponentes pares. Así mismo, la factorización de un número al cubo debe tener sólo exponentes múltiplo de 3. En general un potencia k-ésima perfecta, debe de tener una factorización con exponentes que todos sean múltiplos de k. Por el otro lado, la raíz k-ésima de ese número será el que tiene la factorización con los mismo primos pero cada exponente dividido entre k.
Factorización de un factorial	En los factoriales, contar el número de factores de un primo determinado es sencillo, pues sólo debemos de ver cuántos factores hay en los primeros números enteros. Si estamos analizando a $n!$ en el primo p, esto será igual a un factor p por cada múltiplo de p, luego un factor adicional p en los números que sean divisible por p^2, otro más adicional en los números que sean divisibles entre p^3 y así sucesivamente. Respectivamente, habrá $\left[\frac{n}{p}\right]$ múltiplos de p, $\left[\frac{n}{p^2}\right]$ múltiplos de p^2, $\left[\frac{n}{p^3}\right]$ múltiplos de p^3 y así sucesivamente, donde los corchetes se refieren a la parte entera del número, es decir, la parte sin decimales.

Divisores y múltiplos

MCD y MCM

Divisibilidad

Decimos que a divide a b si pasa alguna de las siguientes situaciones:

1) La división $b \div a$ es exacta y da un número entero
2) La división $b \div a$ deja residuo cero
3) Existe un número k de tal forma que $b = ak$

La definición más correcta y que usaremos preferentemente es la definición número 3.

Usamos el término divisor para el número a y el término múltiplo para el número b, siendo pues a un divisor de b, b un múltiplo de a y también lo podemos decir de la forma b es divisible entre a.

También, utilizamos el símbolo de divisibilidad $a|b$ lo cual se lee y se traduce como a divide a b. Para decir que a no divide a b simplemente se tacha el símbolo.

La divisibilidad entonces tendrá varias propiedades interesantes:

1) **Reflexiva:** $a|a$
2) **Transitiva:** Si $a|b$ y $b|c$, entonces $a|c$
3) **Suma:** Si $a|b$ y $a|c$, entonces $a|b+c$
4) **Resta:** Si $a|b$ y $a|c$, entonces $a|b-c$
5) **Otra versión de Resta:** Si $a|b$ y $a|b+c$, entonces $a|c$
6) **Multiplicación:** Si $a|b$, entonces $a|bc$ para todo entero c
7) **Combinación lineal:** Si $a|b$ y $a|c$, entonces $a|bx+cy$ para cualesquiera enteros x y y

8) **Simetría:** Si $a|b$ y $b|a$, entonces $a = \pm b$
9) **Divisores del cero:** $a|0$ para todo entero a
10) **Divisibles por cero:** $0|a$ sólo cuando $a = 0$
11) **Divisibles por 1:** $1|a$ para todo entero a

Se debe tener cuidado al hablar de divisibilidad entre 0, sin embargo, es posible manejarla usando la definición marcada en el número 3 de las definiciones. Estas definiciones y propiedades de la divisibilidad pueden todas ser demostradas con la definición de divisibilidad, y además nos van a permitir, junto con identidades y trucos algebraicos hacer bastante problemas de divisibilidad generales, a diferencia de los criterios de divisibilidad que se limitan a algunos números.

Identidades algebraicas útiles en Teoría de números

Dentro de las identidades más útiles dentro de los problemas de divisibilidad y teoría de números se encuentran las siguientes:

1) **Diferencia de cuadrados:** $x^2 - y^2 = (x - y)(x + y)$

   Se enuncia así: la diferencia de los cuadrados de dos números, es igual al producto de su suma y de su resta (binomios conjugados).
2) **Binomio al cuadrado:** $(x + y)^2 = x^2 + 2xy + y^2$

   Se enuncia así: El cuadrado de la suma de dos números (binomio) es igual a la suma del cuadrado del primero, más el cuadrado del segundo, más el doble producto de el primero por el segundo.
3) **Diferencia de cubos:** $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$
4) **Diferencia de potencias:** $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + ... + xy^{n-2} + y^{n-1})$
5) **Suma de potencias con exponente impar:**

   $x^{2n+1} + y^{2n+1} = (x + y)(x^{2n} - x^{2n-1}y + x^{2n-2}y^2 - ... - xy^{2n-1} + y^{2n})$

Estas se utilizan frecuentemente durante la manipulación de expresiones para obtener algunas donde tengamos algún factor o sumando que ya sepamos que es divisible entre el número que deseamos o en su defecto sea fácilmente comprobable.

La forma de los números: Residuos y algoritmo de la división

El algoritmo de la división es más que nada el proceso que utilizamos para dividir un número a otro pero haciendo énfasis en el residuo del número. Por ejemplo al dividir el número 2019 entre 6, resulta 336 y sobra 3, esa información se expresa en la siguiente igualdad:

$$2019 = 6 \times 336 + 3$$

El algoritmo general de la división de un número a entre un número b (con $b \neq 0$), nos dice que siempre existirán números enteros q y r (el cociente y el residuo respectivamente) tales que $a = bq + r$ con $0 \leq r < |b|$ donde $|b|$ se refiere al valor absoluto de b.

Este resultado tiene consecuencias importantes, aunque parezca algo trivial.

En particular uno de los usos que se le da principalmente es el clasificar los números acorde a su residuo al dividir entre algún número. Por ejemplo, al dividir entre 5, puede haber números con residuo 0, 1, 2, 3 o 4. Respectivamente, decimos que esos números son de la forma $5k$, $5k + 1$, $5k + 2$, $5k + 3$ y $5k + 4$. Hablar de esa forma, nos permite realizar operaciones con el número de tal forma que el cociente resulta ciertamente irrelevante a la hora de ver la divisibilidad por el número por el cual dividimos, por ejemplo, si tenemos un número de la forma $5k+2$ y quisiéramos demostrar que su cuadrado más uno siempre será divisible por 5, sólo es necesario elevar la expresión de su forma, sumarle uno y verificar que es cierto $(5k+2)^2+1=(25k^2+20k+4)+1=25k^2+20k+5$. Como todos los términos de de esa expresión tienen un factor 5, la expresión siempre será múltiplo de 5 y así habremos demostrado que todos los números de esa forma cumplirán que su cuadrado más uno es múltiplo de 5.

Residuos y congruencias

Hemos hablado ya antes de la divisibilidad y del algoritmo de la división. Ahora bien, con las propiedades de la divisibilidad podemos hacer cosas como sumar dos múltiplos de un número y obtener un número que también será múltiplo, sin embargo, a veces los números o expresiones que consideremos, no serán múltiplos. Analizando su residuo en la división es posible hacer algunas operaciones como la suma, la resta y la multiplicación, de tal forma que el residuo de la suma o producto al dividirlo, será equivalente al residuo de hacer la operación con los residuos (muy parecido a como al sumar o multiplicar y fijarnos sólo en la última cifra, podemos saber la última cifra sin necesidad de calcular todo el número).

Así pues, se inventa como una nueva operación o un esquema en el que las operaciones se puede realizar sólo pensando en el residuo que dejan al dividirse entre el número que estamos considerando. Si estamos dividiendo entre el número n, entonces le llamaremos congruencias módulo n a este sistema de operaciones.

-En general, el residuo de dividir las potencias sucesivas de un número fijo siempre llegarán a un ciclo con un patrón repetitivo como al analizar su última cifra.

Propiedades

-Si el residuo de dividir un número x entre n se denota como $r_n(x)$, entonces:

$$r_n(r_n(x)+r_n(y))=r_n(x+y)$$
$$r_n(r_n(x)\cdot r_n(y))=r_n(x\cdot y)$$

-El criterio de divisibilidad del 3 y del 9 son válidos y más aún al sumar las cifras de un número, el número resultante tendrá el mismo residuo al dividir respectivamente entre 3 y 9 que el original

-El criterio del 11 (sumando las unidades, centenas, decenas de millar, etc. y restando las decenas, las unidades de millar, etc) también nos da una forma de calcular el residuo de el número al dividirlo entre 11

-Si $a\equiv x\ (mod\ n)$ y $b\equiv y\ (mod\ n)$, entonces:

$$a+b\equiv x+y\ (mod\ n)$$
$$ab\equiv xy\ (mod\ n)$$

-En general pueden hacerse suma y resta pensando sólo en el residuo o en números congruentes

-La propiedad general de las congruencias (de hecho es su definición formal)

$$a\equiv b\ (mod\ n) \Leftrightarrow n|a-b$$

Problemas

Ejercicio 1. ¿Cuál es el último dígito de 2010^{2010}? ¿Cuál es el último dígito de 2011^{2011}? ¿Y de 2015^{2015}? ¿Cuál es el último dígito de 2013^{2013}? ¿Cuál es el de $2013^{2013} + 2014^{2014} + 2015^{2015} + 2016^{2016} + 2017^{2017}$?

Ejercicio 2. ¿Es $61^{61} + 71^{71}$ divisible entre 3?

Ejercicio 3. Hay que escribir una fila de 20 dígitos de manera que la suma de tres dígitos consecutivos de la fila sea siempre múltiplo de 5. ¿Cuál es la máxima cantidad de dígitos distintos que puede haber en la fila?

Ejercicio 4. Demuestra que $n^7 - n$ es divisible entre 7 para cualquier entero n.

Ejercicio 5. ¿Cuántas ternas de dígitos (x, y, z) es posible formar, de modo que la suma $x^2 + y^2 + z^2$ sea un múltiplo de 5? (Nota: las ternas $(0,1,3)$, $(1,0,3)$ son diferentes.)

Ejercicio 6. Muestra que $2^{2p} + 2^{2q}$ no puede ser un cuadrado perfecto para p, q enteros positivos.

Ejercicio 7. ¿Puede un número con 2013 dígitos 3, 2013 dígitos 2 y 2013 dígitos 0 en cualquier orden ser un cuadrado perfecto?

Ejercicio 8. Encuentre todos los números primos positivos p tales que $8p^4 - 3003$ también es un primo positivo.

Ejercicio 9. Sea p un número primo tal que $p = p_1^4 + p_2^4 + p_3^4 + p_4^4 + p_5^4$ donde $p_1, \dots, p_5$ son números primos. Muestra que uno de ellos debe ser 5.

Ejercicio 10. Considera los números primos $p_1 < p_2 < \cdots < p_{31}$. Si 30 divide a $p_1^4 + p_2^4 + \cdots + p_{31}^4$, muestra que entre estos números hay tres primos consecutivos.

1) Encuentre todos los enteros n tales que $n - 2|2n$
2) Encuentre todos los enteros n tales que $n - 1|n^2 - 2n$
3) Encuentre todos los enteros n tales que $n - 1|n^2 + 2n$
4) Encuentre el mayor entero positivo n tal que $n^3 + 100$ es divisible entre $n + 10$
5) Demuestra que la fracción $\frac{n+1}{3n+2}$ es irreducible
6) Demuestra que la fracción $\frac{12n+1}{30n+2}$ es irreducible
7) Demuestre que si dos fracciones son irreducibles (es decir, están simplificadas), y su suma da un número entero, entonces, tienen el mismo denominador.
8) Demuestra que $3|4^n - 1$
9) Demuestra que $11|3^{2n+2} + 2^{6n+1}$
10) Demuestra que $17|3^{4n+2} + 2 \cdot 4^{3n+1}$
11) Demuestra que $11|2^{2n-1} \cdot 3^{n+2}$ +1
12) Demuestra que $11|5^{5n+1} + 4^{5n+2} + 3^{5n}$
13) Demuestra que $17|3 \cdot 5^{2n+1} + 2^{3n+1}$
14) Demuestra que para cualquier n, $(n^3 - n)(5^{8n+4} + 3^{4n+2})$ es múltiplo de 3804
15) Encuentra todos los números enteros tales que $3|n^2 + 1$
16) Encuentra todos los números primos que son iguales a la suma de dos números primos y también son iguales a la resta de dos números primos

17) Demuestra que si dos números enteros a y b cumplen que su producto es 12313942398007, entonces uno de ellos es de la forma 4k+1 y el otro de la forma 4q+3.
18) ¿Cuáles son las posibles terminaciones del cuadrado de un número entero?
19) Demostrar que si un número primo es de la forma 3k+1 entonces es de la forma 6k+1
20) Demuestra que un número es divisible por 9 si y sólo si la suma de sus dígitos es divisible por 9 (criterio del 9).
21) Demuestre que $n^3 - n$ es múltiplo de 6 para toda n entera
22) Demuestra que si la suma de los dígitos de un número n es s, entonces $r_9(n) = r_9(s)$
23) Calcula el resto de la división de $(34210987654345664321345 67)^2$ entre 9.
24) Sean a, b y c enteros tales que $a^2 + b^2 = c^2$. Prueba que:
    a) a o b es par
    b) a o b es divisible por 3
    c) a o b o c es divisible por 5
    d) a o b es divisible por 4
25) ¿Cuál es el residuo de dividir 2n entre n-1?
26) ¿Cuál es el residuo de dividir $n^2 - 1$ entre n?
27) Demostrar que 3, 5 y 7 es la única terna de números primos que son impares consecutivos.
28) ¿Cuáles son los posibles residuos de un número primo al dividirlo entre 4? ¿y entre 6?
29) Se sabe que para un número natural n, el número $n^3 + 2009n + 27n$ termina en 3. Encuentra los tres últimos dígitos del número (Sugerencia: “Divide” entre 1000 y observa el residuo, ¿qué pasa si le sumas 27 al residuo?)
30) Encuentra todas los enteros positivos n tales que n divide a $3n + 7$
31) ¿Cuántos números n existen menores o iguales a 2019 tales que el cociente de dividir n entre 100 y el residuo de dividir n entre 100 es múltiplo de 11?
32) Demuestre que si m es un número impar, entonces $2m$ es un número de la forma $4k + 2$.
33) Se tiene un número de la forma $3k + 2$ y de la forma $2q + 1$ al mismo tiempo. ¿Qué residuo deja al dividirlo entre 6?
34) Sea N = 20172017 . . . 2017, el número formado al pegar 2017 veces el 2017. ¿Cuál es el residuo de N al dividirlo entre 3?.
35) Se define la siguiente función f(n)
    a) Si n es un número de la forma 3k, entonces f(n)= $\frac{n}{3}$
    b) Si n es un número de la forma 3k+1, entonces f(n)= $2n + 1$
    c) Si n es un número de la forma 3k+2, entonces f(n)= $2n - 1$

    Demuestre que para todo entero n, se puede llegar al número 1 aplicando sucesivamente la función (es decir, que existe un entero i tal que si aplicamos sucesivamente la función a un número i veces, llegamos al número 1).
36) Demuestre que sin importar qué números enteros naturales sean m y n, el número $mn(m + n)(m-n)$ es divisible siempre por 3.

37) Demuestra que la suma del cuadrado de dos enteros nunca puede dar un número de la forma $4k+3$ o $4k+2$
38) Encuentre todos los números primos p tales que el número $2p+5$ es el cuadrado de un número entero.
39) Demuestra que ningún entero positivo de la forma $8k+7$ puede ser escrito como la suma de tres números cuadrados perfectos
40) Sean p y q dos números primos, demuestre que si $p-q$ es una potencia de 2 mayor a 1, entonces $p+q$ es divisible entre 3.
41) Si a es un número impar, entonces demostrar que a^2-1 es divisible entre 8
42) Si a es un número impar y no es divisible entre 3 ni entre 5, entonces demostrar que $240|a^2-1$
43) Demuestre que 2002^{2002} no puede escribirse como la suma de los cubos de tres números
44) Encontrar todas las soluciones a la ecuación $m^4+m^2=n^4+5$
45) Encuentre todas las soluciones de $1!+2!+3!+...+n!=m^2$
46) Encuentre todas las soluciones enteras a $3^x+7^y=5^z+1$