T.P. (1ra parte): Números pseudoprimos y de Carmichael

El *Pequeño Teorema de Fermat* es un teorema que verán más adelante en la teórica de Álgebra I. Este resultado afirma lo siguiente.

Sea p un número primo positivo. Entonces, para todo número natural a coprimo con p, p divide a $a^{p-1} - 1$.

Como consecuencia de esto, tenemos que para todo primo positivo $p \geq 3$, como 2 es coprimo con p, p divide a $2^{p-1} - 1$. Sin embargo, esta propiedad no es exclusiva de los números primos. Hay algunos números naturales compuestos que también la satisfacen, y ellos se llaman 2-*pseudoprimos*. En otras palabras, los 2-pseudoprimos son los números naturales compuestos n para los cuales n divide a $2^{n-1} - 1$. Los primeros 2-pseudoprimos son 341, 561, 645, 1105, 1387, 1729, 1905, ...

Más en general, dado un número natural a, los *a-pseudoprimos* son los números naturales compuestos n para los cuales n divide a $a^{n-1} - 1$. Los primeros 3-pseudoprimos son 91, 121, 286, 671, 703, 949, 1105, 1541, 1729, ... Los primeros 4-pseudoprimos son 15, 85, 91, 341, 435, 451, 561, 645, 703, ...

Finalmente, los *números de Carmichael* son los números naturales compuestos n que son a-pseudoprimos para todo número natural a entre 1 y $n - 1$ que sea coprimo con n. Es sabido que existen infinitos números de Carmichael, pero aparecen muy espaciadamente dentro de la sucesión de los números naturales. Los únicos números de Carmichael menores a 100.000 son 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973 y 75361. Los números de Carmichael son muy importantes en Teoría de Números, porque si bien no son números primos, pasan algunos test probabilísticos de primalidad que posiblemente verán más adelante en la teórica de Álgebra I.

Esta primera parte del T.P. consiste en programar las siguientes funciones:

• `sonCoprimos :: Integer -> Integer -> Bool`, que dados dos números naturales decide si son coprimos.

• `es2Pseudoprimo :: Integer -> Bool`, que dado un número natural decide si es 2-pseudoprimo.

• `cantidad3Pseudoprimos :: Integer -> Integer`, que dado un número natural m calcula la cantidad de 3-pseudoprimos que hay entre 1 y m inclusive.

• `kesimo2y3Pseudoprimo :: Integer -> Integer`, que dado un número natural k calcula el k-ésimo número que es simuláneamente 2-pseudoprimo y 3-pseudoprimo.

• `esCarmichael :: Integer -> Bool`, que dado un número natural decide si es un número de Carmichael (**esta última función es opcional**).

Aclaraciones importantes:

• Un número natural n es *compuesto* si $n > 1$ y n no es primo (por lo tanto el 1 no es ni primo ni compuesto).

• Si a y n son números naturales, a y n son coprimos si el único divisor positivo que tienen en común es el 1.

• Habrán notado posiblemente que en esta parte del T.P. las funciones utilizan el tipo `Integer` en vez del tipo `Int`, que es el que usamos normalmente en los ejercicios del Taller. Esto es porque es necesario realizar operaciones entre números muy grandes que exceden el rango del tipo `Int` (por ejemplo, para decidir si 561 es un número de Carmichael, el programa debe chequear entre otras cosas si 561 divide a $560^{560} - 1$, que es un número muy grande).

• El T.P. es individual.

• Cada alumno tiene que entregar un único archivo .hs, cuyo nombre esté formado por su apellido, su numero de libreta (sin la barra) y su numero de grupo, separados por guión bajo (sin espacios). Por ejemplo: Fernandez_08420_grupo4.hs.

• Pueden programar todas las funciones auxiliares que consideren necesarias, pero el código de estas funciones debe ser parte de la entrega, incluso si utilizan funciones como por ejemplo `esPrimo` que es parte de la lista de ejercicios de la clase 5. Pueden incluir también, si quieren, breves comentarios para explicar el código. El archivo que entregan tiene que poder compilarse, y sin llamar a otro módulo.

• La fecha y hora límite para la entrega es el Domingo 31 de mayo a las 23:59.

• La entrega se hace subiendo el archivo en el campus. Para poder hacer esto, necesitan estar matriculados en el aula virtual del Taller. Recuerden que **no hace falta ninguna clave para matricularse**.

• Si tienen dudas con respecto al enunciado de esta primera parte del T.P. (es decir, si no les quedan claras las consignas), pueden hacer consultas enviando un mail a la lista de docentes algebra1-doc (arroba) dc.uba.ar. **No hacer consultas en los foros ni mandando mails a la lista de alumnos.**

• Hacia el final del cuatrimestre, intentaremos realizar un coloquio individual en el que cada alumno responda preguntas sobre las funciones que programó en las distintas partes del T.P.

• **Aclaración adicional: No está permitido utilizar en el T.P. la función `gcd` del `Prelude`.**