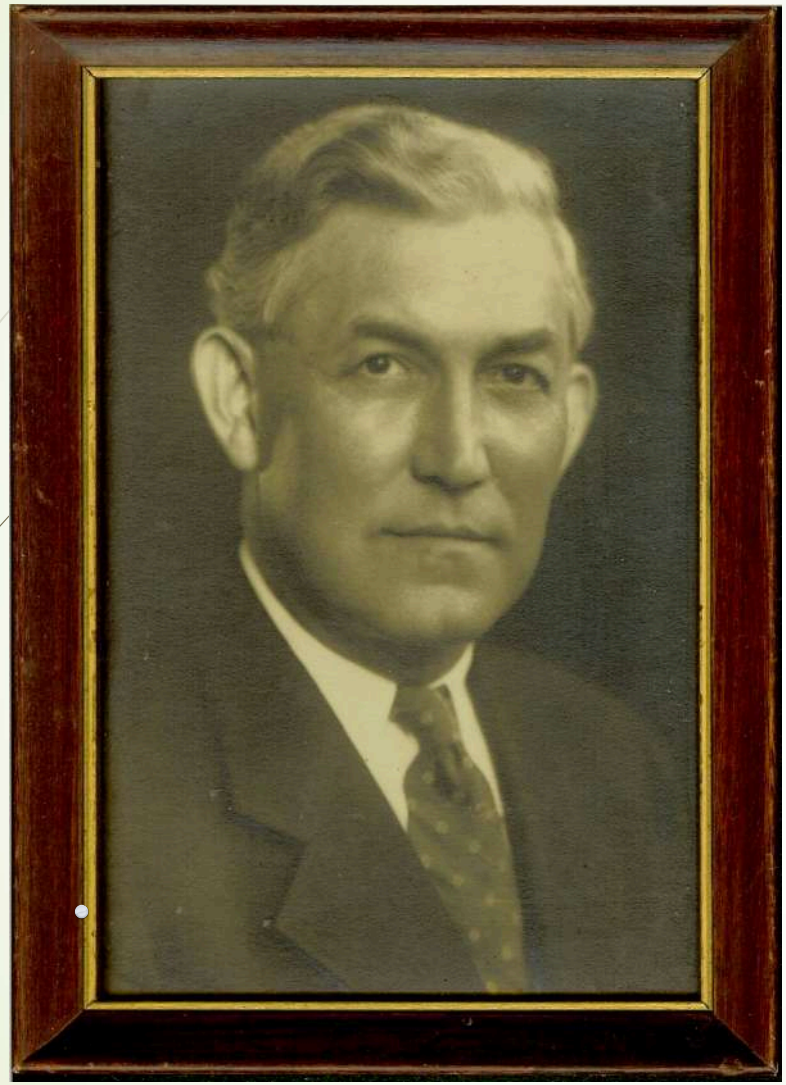
Clase 25

Pseudoprimos y números de Carmichael

- Recordemos que el Pequeño Teorema de Fermat establece que si p es un número primo y a es coprimo con p, entonces $a^{p-1} \equiv 1 \pmod{p}$. Esto da lugar a la siguiente:
- Definición: Pseudoprimo: Dado a > 1 entero, un número entero positivo compuesto n es Pseudoprimo en la base a si: $a^{n-1} \equiv 1 \pmod{n}$.
- Observación: Si n es Pseudoprimo en la base a en particular a es coprimo con n.
- Convención: Si no se especifica la base y se dice simplemente que "n es Pseudoprimo" entendemos que lo es respecto de la base a = 2.

- Es natural preguntarse si un entero n > 1 que cumple la congruencia en la definición anterior para todo a coprimo con n (es decir, que es o primo o Pseudoprimo en base a para todo a coprimo con n) es necesariamente primo. Una respuesta afirmativa significaría que vale el recíproco del Pequeño Teorema de Fermat, pero la respuesta es que no, y esto da lugar a la siguiente:
- Definición: Un entero n > 1 compuesto se dice que es un Número de Carmichael si es Pseudoprimo en la base a para todo a coprimo con n.
- Observación: Los números de Carmichael son "raros", por ejemplo sólo hay 1 menor que 1000, 43 hasta el millón y 8241 hasta el billón. De todos modos, se sabe que son infinitos, de hecho se sabe que la cantidad C(x) de números de Carmichael menores que x es por lo menos $\sqrt[3]{x}$ para todo x suficientemente grande.



Robert Carmichael

- Teorema: Los números de Carmichael tienen las siguientes propiedades:
- (a) Un número de Carmichael n es libre de cuadrados, es decir, para todo primo primo p que divide a n, p^2 no divide a n.
- (b) Sea n un entero mayor que 1, compuesto y libre de cuadrados. Entonces:
- n es de Carmichael $\Leftrightarrow$ para todo primo p con $p \mid n$ se cumple: $p - 1 \mid n - 1$
- (c) Un número de Carmichael posee al menos tres divisores primos.

- Demostración: (a) Razonando por el absurdo, supongamos que se cumple:
- $a^{n-1} \equiv 1 \pmod{n}$ para todo a coprimo con n y $p^2 \mid n$ para un primo p.
- Utilizando la fórmula para $\varphi(n)$ vemos que $p^2 \mid n \Rightarrow p \mid \varphi(n)$.
- Como $a^{n-1} \equiv 1 \pmod{n}$ y $p^2 \mid n \Rightarrow a^{n-1} \equiv 1 \pmod{p^2}$, para todo a coprimo con n. Es fácil ver que de entre los a coprimos con n podemos escoger un valor a_0 que sea raíz primitiva módulo p^2 : de hecho si llamo $p = p_1 , p_2 , \ldots, p_r$ a los factores primos de n basta con coger a_0 solución del sistema:
- $$\begin{cases} x \equiv \boldsymbol{\zeta} \pmod{p^2} \\ x \equiv 1 \pmod{p_2} \ldots \\ x \equiv 1 \pmod{p_r} \end{cases}$$
- Donde $\boldsymbol{\zeta}$ es una raíz primitiva módulo p^2 (por el Teorema Chino de los Residuos, sabemos que el sistema tiene solución).

- Como a_0 es raíz primitiva módulo p^2 , su orden módulo p^2 es $\varphi(p^2) = p(p-1)$.
- Como tenemos que $a_0^{n-1} \equiv 1 \pmod{p^2}$ ⇨ $p(p-1) \mid n-1$, y en particular vemos que $p \mid n-1$, lo cual es absurdo pues $p \mid n$. Esta contradicción prueba que n es libre de cuadrados.
- (b) Sea n libre de cuadrados, es decir, se tiene la descomposición en primos diferentes: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Suponemos que n es compuesto, es decir, $r > 1$.
- Supongamos que n es de Carmichael, es decir, que $a^{n-1} \equiv 1 \pmod{n}$ para todo a coprimo con n. En particular: $a^{n-1} \equiv 1 \pmod{p_i}$. Con el mismo argumento que ya usamos en el apartado (a) vemos que de entre los a coprimos con n podemos escoger a que sea raíz primitiva módulo p_i ⇨ el orden de a módulo p_i es $p_i - 1$. Luego, como $a^{n-1} \equiv 1 \pmod{p_i}$ tenemos que $p_i - 1 \mid n - 1$.

- Recíprocamente: supongamos que para todo p_i primo que divide a n se cumple $p_i - 1 \mid n - 1$. Sea a coprimo con n (ergo, no es divisible por ninguno de los p_i). Por el Pequeño Teorema de Fermat $a^{p_i - 1} \equiv 1 \ (mod \ p_i)$. De aquí, como $n - 1 = k_i \cdot (p_i - 1)$ para ciertos enteros $k_i \Rightarrow a^{n-1} \equiv 1 \pmod{p_i}$ para todo i = 1,2, ….,r.
- Como $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r \Rightarrow a^{n-1} \equiv 1 \pmod{n}$, ∀ a coprimo con n.
- (c) Sea n un número de Carmichael. Podemos suponer (apartado (a)) que n es libre de cuadrados. Supongamos que n posee sólo dos divisores primos, es decir, que $n = p \cdot q$, con p y q primos distintos. Supondremos que $p < q$.
- Por el apartado (b) sabemos que $q - 1 \mid n - 1$. Por otro lado:
- $n - 1 = p \cdot q - 1 = p \cdot q - p + p - 1 = p \cdot (q - 1) + p - 1 \equiv p - 1 \pmod{(q - 1)}$.
- Es decir que: $n - 1 \equiv 0 \pmod{(q - 1)}$ y $n - 1 \equiv p - 1 \pmod{(q - 1)} \Rightarrow$
- $p - 1 \equiv 0 \pmod{(q - 1)} \Rightarrow q - 1 \mid p - 1$, pero esto es absurdo pues $p - 1 < q - 1$.
- Esto prueba que todo número de Carmichael posee al menos 3 divisores primos.

- Ejemplos de Números de Carmichael:
- $561 = 3 \cdot 11 \cdot 17$
- $1105 = 5 \cdot 13 \cdot 17$
- $1729 = 7 \cdot 13 \cdot 19$
- $41041 = 7 \cdot 11 \cdot 13 \cdot 41$
- Observación: Para verificar que un entero compuesto n es un número de Carmichael basta con verificar que $a^{n-1} \equiv 1 \pmod{n}$ para todo a coprimo con n en el intervalo [2, n-1]. Un entero que satisfaga todas estas congruencias será o bien primo o bien Carmichael. Este será el punto de partida de algunos criterios de primalidad que veremos más adelante.

Clase 26

Tests de Primalidad

- Basándonos en varios de los resultados de la teoría de congruencias y símbolos cuadráticos, veamos ahora algunos tests de primalidad, es decir, algoritmos determinísticos o probabilísticos para determinar si un número es (o tiene alta probabilidad de ser) primo.
- Si sólo utilizáramos la definición, sería preciso probar la división entre un número n y todos los números anteriores para concluir que n es primo en el caso en que no posea ningún divisor no trivial. Pero esto es muy lento, pues implica realizar n divisiones. Si utilizáramos por ejemplo el criterio dado por el Teorema de Wilson (y su recíproco) deberíamos chequear que $(n-1)! \equiv -1 \pmod{n}$ para concluir que un $n > 1$ es primo. Esto también es muy lento pues calcular $(n-1)!$ requiere hacer $n - 2$ multiplicaciones, y si bien es conveniente para reducir la complejidad (y trabajar con números acotados por n^2) reducir módulo n tras cada multiplicación, de todos modos son muchas multiplicaciones.
-

- Si intentáramos usar como criterio de primalidad el Pequeño Teorema de Fermat, deberíamos verificar que para todo a en el intervalo [2, n-1] coprimo con n se tiene $a^{n-1} \equiv 1 \pmod{n}$. Un número que cumpla todos estos requisitos es o bien primo o bien Carmichael, con lo cual por ser los Carmichael "raros" es probable que n sea primo. De todos modos chequear la congruencia anterior para todos los valores de a especificados requiere $\varphi(n)$ exponenciaciones módulo n, y esto de nuevo es un número muy grande. Una opción razonable es chequear la congruencia $a^{n-1} \equiv 1 \pmod{n}$ sólo para "pocos" valores de a, por ejemplo para $a \leqq \log n$. Esto ya supone un algoritmo razonablemente rápido (utilizando exponenciación binaria para calcular las potencias de a módulo n) y si n cumple las congruencias será Pseudoprimo en base a para todo $a \leqq \log n$, o primo, con lo cual es probable que sea primo.

- Los algoritmos que veremos se basan en ideas similares, pero cambiando la congruencia $a^{n-1} \equiv 1 \pmod{n}$ por condiciones más fuertes que veremos que admiten teoremas conversos, es decir, que son tales que sólo se cumplen para toda base a coprima con n si n es primo. El hecho de que no utilicemos la congruencia $a^{n-1} \equiv 1 \pmod{n}$ como criterio de primalidad se debe a la existencia de los números de Carmichael.

- Test de Solovay-Strassen: Sea n > 1, n impar. Son equivalentes:
- (i) n es primo
- (ii) $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ para todo a coprimo con n.
- Demostración: (i) $\Longrightarrow$ (ii): es el criterio de Euler.
- (ii) $\Longrightarrow$ (i) Supongamos, razonando por el absurdo, que n es compuesto. Si a coprimo con n tenemos que $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ de donde, elevando al cuadrado vemos que $a^{n-1} \equiv 1 \pmod{n}$, luego n es un número de Carmichael. Por las propiedades ya vistas para estos números, sabemos que $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ con los p_i primos impares diferentes y $r \geqq 3$.

- Sea a un entero coprimo con p_1 tal que $\left(\frac{a}{p_1}\right)$ = -1. Si planteamos el sistema de congruencias:
- $\begin{cases} x \equiv a \ (mod\ p_1) \\ x \equiv 1 \ (mod\ p_2) \ \ldots\ldots \\ x \equiv 1 \ (mod\ p_r) \end{cases}$
- Sabemos (Teorema Chino de los Residuos) que existe una solución x_0 con $1 \leqq x_0 \leqq n$. Además como a es coprimo con p_1 vemos que x_0 es coprimo con todos los p_i (pues todos los residuos del sistema son coprimos con los correspondientes módulos), luego $mcd(x_0, n) = 1$.
- Por lo tanto, podemos calcular el símbolo de Jacobi:

- Por lo tanto, podemos calcular el símbolo de Jacobi:
- $\left(\frac{x_0}{n}\right) = \left(\frac{x_0}{p_1}\right) \cdot \left(\frac{x_0}{p_2}\right) \cdot \ldots\ldots \cdot \left(\frac{x_0}{p_r}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{1}{p_2}\right) \cdot \ldots\ldots \cdot \left(\frac{1}{p_r}\right) = (-1) \cdot 1 \cdot 1 \cdot \ldots\ldots \cdot 1 = -1.$
- Por hipótesis $x_0^{\frac{n-1}{2}} \equiv \left(\frac{x_0}{n}\right) \equiv -1 \pmod{n}$ ⇨ en particular $x_0^{\frac{n-1}{2}} \equiv -1 \pmod{p_2}$, pero por otro lado $x_0 \equiv 1 \pmod{p_2}$ por ser solución del sistema de congruencias, y esto implica que $x_0^{\frac{n-1}{2}} \equiv 1 \pmod{p_2}$. De esta contradicción deducimos que si n cumple (ii) entonces n es necesariamente primo.

- Robert Solovay

- Volker Strassen

- A partir de este criterio podemos asegurar que un número impar mayor que 1 que cumple (ii) es primo, pero el problema es que verificar (ii) requiere demasiados cálculos, pues habría que chequearlo para todos los valores de a en el intervalo [1,n] coprimos con n.
- De todos modos, el hecho de tener un criterio de primalidad permite extraer de aquí un test eficiente probabilístico que permite afirmar con una probabilidad razonablemente alta que un número es primo. Enunciemos (sin demostración) esta versión probabilística:
- Test Probabilístico de Solovay-Strassen: Sea n > 1 entero impar. Sean a_1 , a_2 , …., a_k números diferentes todos coprimos con n, en el intervalo [1,n]. Entonces, si se tiene que $a_i^{\frac{n-1}{2}} \equiv \left(\frac{a_i}{n}\right)$ (mod n) para todo i =1,2,….,k, la probabilidad de que n sea primo es mayor o igual que 1 - $\frac{1}{2^k}$.