Clase 27

- Definición: Pseudoprimo de Euler: Sea n un número compuesto e impar. Sea a coprimo con n. Decimos que n es Pseudoprimo de Euler respecto de la base a si: $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)$ (mod n) .
- Observación: Tal como vimos durante la prueba del test de Solovay-Strassen, si n es Pseudoprimo de Euler respecto de a también es Pseudoprimo respecto de a, y no existen números que sean Pseudoprimos de Euler respecto a toda base a coprima con n.
- Definición: Sea n un número impar y compuesto, de donde n-1 = $2^e \cdot t$ con t impar y e > 0. Sea a coprimo con n. Decimos que n es Pseudoprimo Fuerte respecto de a si se verifica que:
- $a^t \equiv 1$ (mod n) o $a^{2^i \cdot t} \equiv -1 \ (mod\ n)$ para algún i ∈ {0, 1, …, e-1}

- Proposición: Si n es Pseudoprimo Fuerte respecto de una base a, entonces es Pseudoprimo de Euler respecto de a.
- Demostración: Dividimos la prueba en 3 casos:
- (i) Supongamos que $a^t \equiv 1 \pmod n$ ⇨ $a^{\frac{n-1}{2}} \equiv a^{2^{e-1}\cdot t} \equiv 1\ (mod\ n)$.
- Calculemos $\left(\frac{a}{n}\right)$: Sabemos que $\left(\frac{a^t}{n}\right) = \left(\frac{1}{n}\right) = 1$ y también que $\left(\frac{a^t}{n}\right) = \left(\frac{a}{n}\right)^t$ por lo tanto $\left(\frac{a}{n}\right)^t = 1$ y como t es impar ⇨ $\left(\frac{a}{n}\right) = 1$.
- Luego, tenemos: $a^{\frac{n-1}{2}} \equiv 1 \equiv \left(\frac{a}{n}\right)\ (mod\ n)$.

- (ii) Supongamos que $a^{2^{e-1}\cdot t} \equiv -1\ (mod\ n)$ ⇨ $a^{\frac{n-1}{2}} \equiv a^{2^{e-1}\cdot t} \equiv -1\ (mod\ n)$.
- Veamos ahora que $\left(\frac{a}{n}\right)$ = -1. Pero antes, unos preliminares:
- Sea p primo tal que p | n (por lo tanto, p impar) y escribamos: p-1 = $2^{e'} \cdot s$ con s impar y e' > 0. Queremos ver que:
- (a) e' ≧ e
- (b) $\left(\frac{a}{p}\right) = \begin{cases} -1 & si\ \ e' = e \\ 1 & si\ \ e' > e \end{cases}$
- (a) $a^{2^{e-1}\cdot t} \equiv -1\ (mod\ n)$ ⇨ $a^{2^{e-1}\cdot t\cdot s} \equiv -1\ (mod\ n)$ ⇨ $a^{2^{e-1}\cdot t\cdot s} \equiv -1\ (mod\ p)$.
- Supongamos que e' < e ⇨ e' ≦ e-1 ⇨ $a^{2^{e'}\cdot t\cdot s} \not\equiv 1\ (mod\ p)$ ⇨ $a^{p-1} \equiv a^{2^{e'}\cdot s} \not\equiv 1\ (mod\ p)$ contradiciendo el Pequeño Teorema de Fermat. Luego e' ≧ e.

- (b) Si e' = e: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv a^{2^{e'-1}\cdot s} \equiv a^{2^{e-1}\cdot s}$ (mod p). Como este símbolo de Legendre (siendo a coprimo con p) vale ± 1 , su valor no cambia si lo elevamos a la t (pues t es impar), luego: $\left(\frac{a}{p}\right) \equiv a^{2^{e-1}\cdot s} \equiv a^{2^{e-1}\cdot s\cdot t} \equiv$ -1 (mod p) (la última congruencia ya fue probada en la parte (a)).
- Si e' > e: Como $a^{2^{e-1}\cdot t} \equiv$ -1 (mod n) elevamos a la s (y cambiamos el módulo por p): $a^{2^{e-1}\cdot s\cdot t} \equiv$ -1 (mod p) ⇨ $a^{2^{e'-1}\cdot s\cdot t} \equiv$ 1 (mod p). Por el criterio de Euler $\left(\frac{a}{p}\right)$ $\equiv a^{\frac{p-1}{2}} \equiv a^{2^{e'-1}\cdot s}$ (mod p). Como $\left(\frac{a}{p}\right)$ = ± 1, su valor no cambia al elevarlo a la t ⇨ $\left(\frac{a}{p}\right) \equiv a^{2^{e'-1}\cdot s} \equiv a^{2^{e'-1}\cdot s\cdot t} \equiv$ 1 (mod p) .

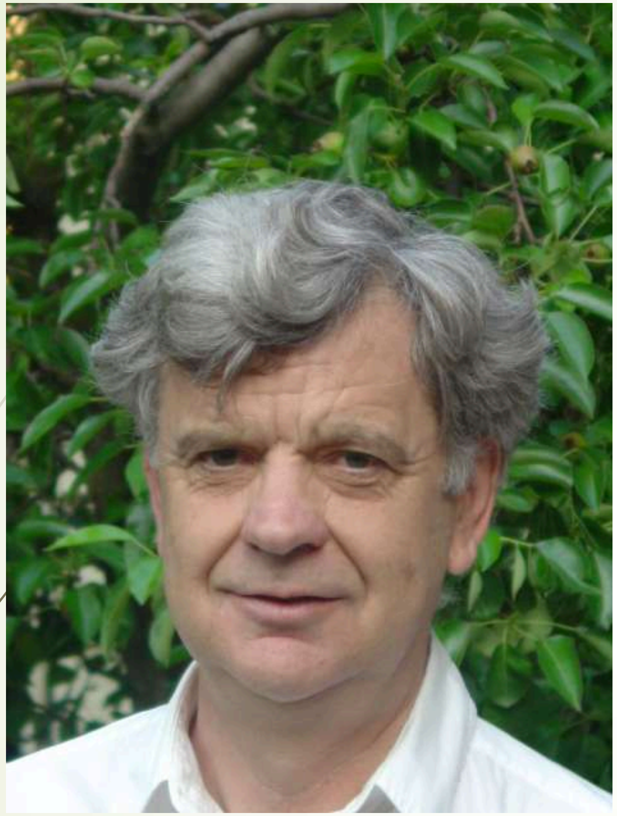
- Volvamos ahora sí al cálculo de $\left(\frac{a}{n}\right)$. Escribimos: n = $\prod_{p|n} p$ (primos no necesariamente distintos). Luego: $\left(\frac{a}{n}\right) = \prod_{p|n} \left(\frac{a}{p}\right) = (-1)^k$ donde k es el número de factores primos de n tales que $\left(\frac{a}{p}\right) = -1$, que por los resultados preliminares (a) y (b) sabemos que k es igual a la cantidad de factores primos de n con e' = e (siempre contando multiplicidades).
- Queremos probar que k es impar, y así: $\left(\frac{a}{n}\right) = (-1)^k = -1 \equiv a^{\frac{n-1}{2}}$ (mod n) .
- Observemos que: e' > e ⇨ $p \equiv 1 \pmod{2^{e+1}}$, y e' = e ⇨ $p \equiv 1 + 2^e \pmod{2^{e+1}}$. Utilizando esto, nos queda:
- $1 + 2^e \equiv 1 + 2^e \cdot t \equiv n \equiv \prod_{p|n} p \equiv (1 + 2^e)^k \equiv 1 + k \cdot 2^e \pmod{2^{e+1}}$ ⇨
- $2^e \cdot (k-1) \equiv 0 \pmod{2^{e+1}}$ ⇨ k-1 par ⇨ k impar, que es lo que queríamos.

Clase 28

- (iii) Supongamos que $a^{2^{i}\cdot t} \equiv -1\ (mod\ n)$ con i ∊ {0, 1, …, e-2}.
- Como i ≦ e – 2 < e – 1 tenemos: $a^{\frac{n-1}{2}} \equiv a^{2^{e-1}\cdot t} \equiv 1$ (mod n).
- Para calcular $\left(\frac{a}{n}\right)$, como en el caso (ii), son necesarios resultados preliminares. Si p primo (impar) que divide a n y p – 1= $2^{e'}$ · s, s impar y e' > 0, se puede ver que se cumplen:
- (a) e' ≧ i + 1
- (b) $\left(\frac{a}{p}\right) = \begin{cases} -1 & si\ \ e' = i+1 \\ 1 & si\ \ e' > i+1 \end{cases}$
- La demostración de estas dos propiedades (que no haremos) utiliza argumentos similares a los vistos en el caso (ii).
-

- Escribamos n = $\prod_{p|n} p$ (primos no necesariamente distintos). Luego: $\left(\frac{a}{n}\right)$ = $\prod_{p|n} \left(\frac{a}{p}\right)$ = $(-1)^k$ donde k es el número de factores primos de n tales que $\left(\frac{a}{p}\right) = -1$, que por los resultados preliminares (a) y (b) sabemos que k es igual a la cantidad de factores primos de n con e' = i+1 (siempre contando multiplicidades).
- Queremos probar que k es par, y así: $\left(\frac{a}{n}\right) = (-1)^k = 1 \equiv a^{\frac{n-1}{2}}$ (mod n) .
- Observemos que: e' > i+1 ⇨ p ≡ 1 (mod 2^{i+2}), y e' = i+1 ⇨ p ≡ 1 + 2^{i+1} (mod 2^{i+2}).
- Como n = 1 + $2^e \cdot t$ y i+2 ≦ e ⇨ n ≡ 1 (mod 2^{i+2}). Luego:
- 1 ≡ n ≡ $\prod_{p|n} p$ ≡ $(1 + 2^{i+1})^k$ ≡ 1 + k · 2^{i+1} (mod 2^{i+2}) ⇨
- $2^{i+1} \cdot k \equiv 0$ (mod 2^{i+2}) ⇨ k par, luego $\left(\frac{a}{n}\right)$ = 1, que es lo que queríamos probar.

- Test de Miller-Rabin: Si n > 1 e impar que satisface la propiedad en la definición de Pseudoprimo Fuerte para toda base a coprima con n (excepto por la condición de ser compuesto). Entonces n es primo.
- Demostración: Por la proposición anterior, n cumple $\left(\frac{a}{n}\right) \equiv \; a^{\frac{n-1}{2}}$ (mod n) para todo a coprimo con n, luego, por el test de Solovay-Strassen, n es primo.
- Observación: Es fácil ver que el recíproco es cierto, es decir, que un número primo cumple con las congruencias en la definición de Pseudoprimo Fuerte en base a para cualquier a coprimo con él. Esto se desprende del Pequeño Teorema de Fermat y de que la congruencia $x^2 \equiv 1$ (mod p) sólo posee las soluciones 1 y -1.



Gary Miller

Michael Rabin

- Observación: En el año 2002 por primera vez se dio con un algoritmo determinístico y polinomial (en log n) para determinar si un entero n es primo o no. Este algoritmo se conoce como el Test de Primalidad AKS, y sus autores son Manindra Agrawal, Neeraj Kayal y Nitin Saxena.

Ternas Pitagóricas

- Veamos para acabar el curso un ejemplo de ecuación diofántica no lineal, en 3 variables, que puede resolverse con técnicas elementales:
- Nos proponemos hallar todas las soluciones en enteros positivos de la ecuación:
- $$x^2 + y^2 = z^2 \qquad (😇)$$
- Estas soluciones reciben el nombre de "Ternas Pitagóricas" pues por el Teorema de Pitágoras sabemos que dan lugar a un triángulo rectángulo de lados enteros. Un ejemplo es la solución (3, 4, 5) pues se tiene que:
- $$3^2 + 4^2 = 9 + 16 = 25 = 5^5$$
- Para comenzar observemos que si x, y, z son enteros positivos solución de (😇) y si $d = \mathrm{mcd}(x, y, z)$ entonces podemos escribir $x = d \cdot X$, $y = d \cdot Y$, $z = d \cdot Z$ con X, Y, Z enteros positivos tales que $\mathrm{mcd}(X, Y, Z) = 1$ y vemos que:
- $(d \cdot X)^2 + (d \cdot Y)^2 = (d \cdot Z)^2 \Rightarrow X^2 + Y^2 = Z^2$.

- Por lo tanto para encontrar todas las soluciones de (😇) está claro que es suficiente con hallar todas aquellas soluciones X, Y, Z con mcd(X, Y, Z) = 1, y a partir de ellas con tan sólo multiplicar a los tres enteros por un entero k arbitrario se obtienen todas las soluciones de la ecuación.
- A una solución (X, Y, Z) con la propiedad mcd(X, Y, Z) = 1 se la llama Solución Primitiva. A partir de ahora veremos como calcular todas las soluciones primitivas de (😇). Sea por lo tanto (X, Y, Z) una tal solución.
- Veamos que se tiene que cumplir también que mcd(X, Y) = mcd(X, Z) = mcd(Y, Z) = 1. Probemos sólo mcd(X, Y) = 1, el resto se prueba con idéntico argumento. Si llamo d = mcd(X, Y) entonces de la ecuación (😇) obtenemos que: $0 \equiv X^2 + Y^2 \equiv Z^2 \pmod{d}$, es decir que d también divide a Z^2. Si suponemos que d > 1, entonces hay al menos un primo p que divide a d, y en particular vemos que p divide a X, Y y Z. Esto contradice la hipótesis de que la terna X, Y, Z es primitiva, con lo cual queda probado que mcd(X, Y) = 1.

- Por lo tanto en una solución primitiva X, Y, Z los elementos son coprimos dos a dos.
- Veamos ahora que X e Y tienen diferente paridad: no pueden ser ambos pares puesto que sabemos que son coprimos, y si fueran ambos impares podemos reducir la ecuación (😇) módulo 4 y obtenemos:
- $2 \equiv X^2 + Y^2 \equiv Z^2 \pmod 4$, lo cual es una contradicción puesto que un cuadrado módulo 4 sólo puede caer en la clase del 0 o en la del 1.
- Ahora que sabemos que X e Y tienen diferente paridad podemos suponer que X es par y que Y es impar (pues la ecuación es simétrica en X e Y), y evidentemente Z tiene que ser impar.
- Como $Z - Y$ y $Z + Y$ son ambos pares, podemos introducir nuevas variables:
- $Z - Y = 2 \cdot s$, $Z + Y = 2 \cdot r$ para r, s enteros.

- Deshaciendo el cambio de variables, vemos fácilmente que se tiene:
- $Y = r - s, \quad Z = r + s \qquad (\#)$
- Veamos que estas nuevas variables r y s tiene que ser números coprimos y de diferente paridad: Si hubiera un divisor común $d > 1$ entre r y s vemos de las fórmulas (#) que d divide a Y y a Z, contradiciendo el hecho de que los elementos de la terna X, Y, Z son dos a dos coprimos. También se deduce de (#) que como Y y Z son impares r y s tienen diferente paridad.
- Como X es par, podemos escribir $X = 2 \cdot W$, con W entero. Sustituyendo las variables X, Y, Z por las variables W, r y s en la fórmula (😇) obtenemos:
- $X^2 = Z^2 - Y^2 \Rightarrow 4 \cdot W^2 = (Z - Y) \cdot (Z + Y) = 4 \cdot r \cdot s$, de donde:
- $W^2 = r \cdot s$. Como sabemos además que r y s son coprimos ⇨ Existen enteros u y v con: $r = u^2$, $s = v^2$ y $W = u \cdot v$. Nótese que como r y s son de diferente paridad, u y v son de diferente paridad.

- Queda probado que cualquier (hipotética) solución primitiva X, Y, Z de (😇) será de la forma:
- $$X = 2 \cdot u \cdot v, \quad Y = u^2 - v^2, \quad Z = u^2 + v^2 \qquad (*)$$
- para enteros positivos u y v que son coprimos y de diferente paridad.
- Veamos finalmente que cualquier terna X, Y, Z obtenida como en (*) de una pareja de enteros positivos u y v coprimos y de diferente paridad, y tales que $u > v$, es una terna de enteros positivos que es solución primitiva de (😇). Para probar que es solución basta con verificar la identidad:
- $(2 \cdot u \cdot v)^2 + (u^2 - v^2)^2 = (u^2 + v^2)^2$, que sale fácilmente aplicando la fórmula del cuadrado de un binomio. Falta con verificar que es primitiva, y para ello veremos que no hay ningún factor primo p en común entre X, Y y Z.

- Supongamos (razonando por el absurdo) que existe un primo p que divide a X, Y y Z. Como Y y Z son impares, tenemos que $p > 2$. Por lo tanto, como p divide a $X = 2 \cdot u \cdot v$ tenemos que p divide a u o a v. Supondremos que p divide a u (el otro caso es análogo). Como p divide a u y también divide a $Z = u^2 + v^2$ tenemos que p divide a $v^2 = Z - u^2$ y por lo tanto que p divide a v. Pero u y v son coprimos, con lo cual no pueden ser ambos múltiplos de p. Esta contradicción prueba que ningún primo puede dividir a X, Y y Z, con lo cual la terna X, Y, Z como en (*) es una solución primitiva de (😇).
- Finalmente, recordemos que para obtener la solución general de (😇), basta con multiplicar por un entero $k > 0$ a las soluciones primitivas. Por lo tanto, la solución general de (😇) es:
- $$X = 2 \cdot k \cdot u \cdot v, \quad Y = k \cdot (u^2 - v^2), \quad Z = k \cdot (u^2 + v^2)$$
- con $k > 0$ y u, v enteros coprimos y de diferente paridad, con $u > v$.