Clase 15

- Proposición: Si p es primo impar y m = 2p, existen raíces primitivas módulo m.
- Demostración: Comenzamos por calcular $\varphi(m) = \varphi(2p) = \varphi(2)\cdot\varphi(p) = \varphi(p) = p-1$. Buscamos por lo tanto un elemento de orden p-1 módulo m.
- Sea a una raíz primitiva módulo p. Como también a+p es raíz primitiva módulo p y alguno de estos dos números es impar, vemos que existe un número b en en intervalo [1, 2p] que es impar y es raíz primitiva módulo p.
- Claramente este b es coprimo con m=2p y por el Teorema de Euler cumple:
- $b^{\varphi(2p)} \equiv b^{p-1} \equiv 1 \pmod{2p}$
- Además como b es raíz primitiva módulo p, tiene orden p-1 módulo p, luego si $1 \leqq e < p-1$:
- $b^e \not\equiv 1 \pmod{p} \implies b^e \not\equiv 1 \pmod{2p}$. Por lo tanto el orden de b módulo m=2p es $p-1 = \varphi(m)$.

- Además de todos los resultados anteriores, también puede verse que si p es un primo impar y r > 0 entonces existen raíces primitivas módulo p^r , es decir, clases inversibles módulo p^r cuyo orden es $\varphi(p^r) = (p-1) \cdot p^{r-1}$. Este resultado lo hemos probado sólo en el caso r=1.
- Como conclusión, se obtiene el criterio que ya hemos mencionado, recordémoslo:
- Criterio: Existen raíces primitivas módulo m > 0 sí y sólo sí m es igual a:
- 1, 2, 4, p^r o $2 \cdot p^r$, con $r \geqq 1$, donde p es un primo impar.

Residuos Cuadráticos y Ley de Reciprocidad Cuadrática

- Sea p primo. Para cada entero a no divisible por p planteamos la congruencia cuadrática:
- $x^2 \equiv a \pmod{p}$ (💙)
- Observaciones:
- (1) En el caso a divisible por p, es decir, $a \equiv 0 \pmod{p}$, esta congruencia tiene la solución trivial $x \equiv 0 \pmod{p}$.
- (3) El problema (como toda congruencia!) sólo depende de la clase de congruencia de a módulo p.
- Definición: Si existe solución de la ecuación (💙) decimos que a es un residuo cuadrático módulo p. En caso contrario, decimos que a es un no-residuo cuadrático módulo p.

- Proposición: Sea p primo impar. De las p-1 clases residuales módulo p diferentes de la del 0, (p-1)/2 son residuos cuadráticos y (p-1)/2 no-residuos cuadráticos. Más precisamente, si $\boldsymbol{\alpha}$ es una raíz primitiva módulo p, y por lo tanto:
- $\boldsymbol{\alpha}, \boldsymbol{\alpha}^2, \ldots, \boldsymbol{\alpha}^{p-1}$ recorren las p-1 clases inversibles módulo p, se tiene que:
- $\boldsymbol{\alpha}^k$ es residuo cuadrático módulo p $\Leftrightarrow$ k es par
- Demostración: Si k es par, es decir, $k = 2 \cdot w$, se tiene que $\boldsymbol{\alpha}^k = (\boldsymbol{\alpha}^w)^2$ es un cuadrado, con lo cual la congruencia $\boldsymbol{\alpha}^k \equiv x^2 \pmod p$ tiene la solución $x = \boldsymbol{\alpha}^w$, es decir, $\boldsymbol{\alpha}^k$ es residuo cuadrático módulo p. De este modo hemos obtenido (p-1)/2 clases residuales módulo p que son residuos cuadráticos, pues hay (p-1)/2 números pares en el intervalo [1, p-1].

- Como ya tenemos (p-1)/2 residuos cuadráticos, queda sólo por ver que el número de (clases inversibles correspondientes a) residuos cuadráticos es exactamente (p-1)/2. Esto probará en particular que α^k es residuo cuadrático SOLAMENTE cuando k es par.
- Si β es residuo cuadrático, existe un z (también inversible) tal que $\beta \equiv z^2 \pmod{p}$. Luego:
- $\beta^{\frac{p-1}{2}} \equiv (z^2)^{\frac{p-1}{2}} \equiv z^{p-1} \equiv 1 \pmod{p}$, por el pequeño Teorema de Fermat.
- Por lo tanto β es solución de la congruencia $y^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Por el teorema de Lagrange, esta congruencia no puede tener más de (p-1)/2 soluciones, con lo cual concluimos que no puede haber más de (p -1)/2 residuos cuadráticos.

- Proposición (Criterio de Euler): Sea p primo impar y a un entero no divisible por p. Entonces:
- $$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \ si\ a\ es\ residuo\ cuadrático\ módulo\ p \\ -1\ si\ a\ es\ noresiduo\ cuadrático\ módulo\ p \end{cases}$$
- Demostración: Por el pequeño Teorema de Fermat:
- Sea b = $a^{\frac{p-1}{2}}$ ⇨ $b^2 \equiv a^{p-1} \equiv 1 \pmod p$. Luego b = $a^{\frac{p-1}{2}}$ es solución de la congruencia cuadrática: $x^2 \equiv 1 \pmod p$. Sabemos que esta congruencia tiene SÓLO dos soluciones: $x \equiv 1 \pmod p$ y $x \equiv -1 \pmod p$. Por lo tanto:
- $$a^{\frac{p-1}{2}} \equiv \pm 1 \ (mod\ p) \qquad (\#)$$

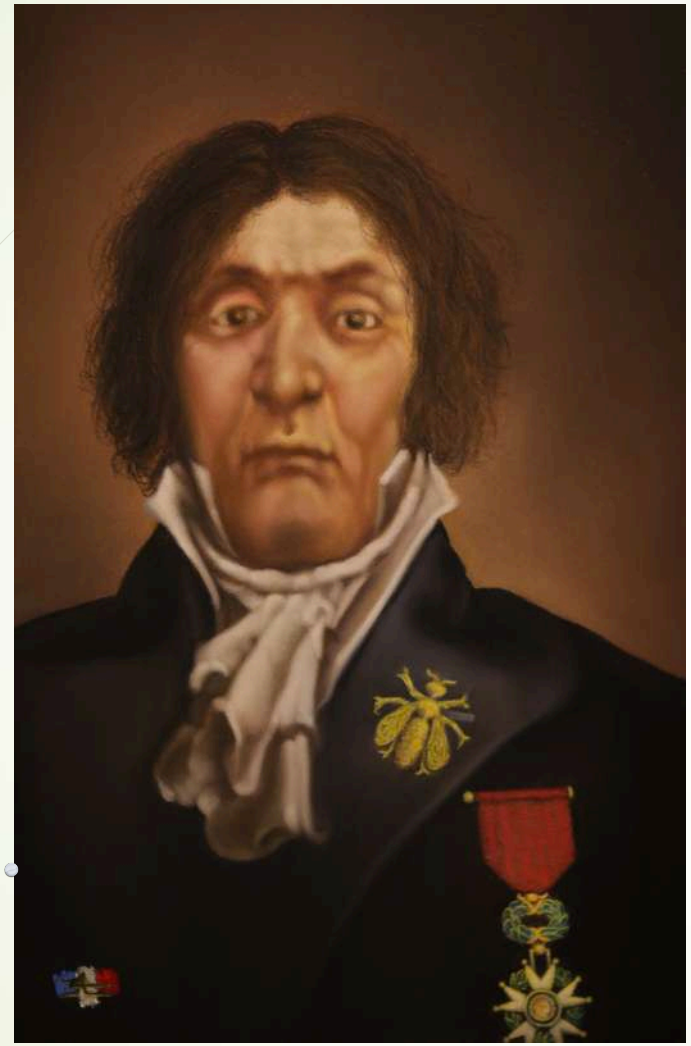
- Si a es residuo cuadrático módulo p: $a \equiv u^2 \pmod{p}$ para algún entero u, luego: $a^{\frac{p-1}{2}} \equiv u^{p-1} \equiv 1 \pmod{p}$, por el pequeño Teorema de Fermat. Tenemos por lo tanto (p-1)/2 clases residuales, aquellas correspondientes a residuos cuadráticos, que resuelven la congruencia $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, y como sabemos por el Teorema de Lagrange que esta congruencia no puede tener más de (p-1)/2 soluciones, concluimos que para todo no-residuo cuadrático β se tiene: $\beta^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, y por lo tanto de (#) deducimos que para un tal β se tiene: $\beta^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

- Definición: Símbolo de Legendre: Si p es un primo impar y a un entero definimos el Símbolo de Legendre $\left(\frac{a}{p}\right)$ como:
- $\left(\frac{a}{p}\right) = \begin{cases} 0 \quad si\ p\ divide\ a\ a \\ 1 \ si\ p\ no\ divide\ a\ a\ y\ a\ es\ residuo\ cuadrático\ módulo\ p \\ -1 \quad si\ p\ no\ divide\ a\ a\ y\ a\ es\ no-residuo\ cuadrático\ módulo\ p \end{cases}$
- Propiedades:
- (i) a ≡ b (mod p) $\Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- (ii) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ (mod p), si p es primo impar
- (iii) $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
- (iv) Si p no divide a c $\Longrightarrow \left(\frac{c^2 \cdot b}{p}\right) = \left(\frac{b}{p}\right)$

- Demostración:
- (i) Tal como ya observamos, ser o no ser residuo cuadrático sólo depende de la clase de congruencia módulo p (y lo mismo para ser divisible por p).
- (ii) Si a es divisible por p, $a^{\frac{p-1}{2}}$ también, y la congruencia en este caso es
- $0 \equiv 0 \pmod{p}$. Si a no es divisible por p, esta congruencia equivale al Criterio de Euler (de hecho, es común que se formule el Criterio de Euler usando el Símbolo de Lagrange).
- (iii) Se deduce fácilmente de (ii):
- $\left(\frac{a \cdot b}{p}\right) \equiv (a \cdot b)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod{p}$
- (iv) Sale de (iii), pues: $\left(\frac{c^2 \cdot b}{p}\right) = \left(\frac{c^2}{p}\right) \cdot \left(\frac{b}{p}\right) = 1 \cdot \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)$, donde hemos utilizado el hecho de que c^2, por ser un cuadrado y no ser divisible por p, es residuo cuadrático módulo p.

Clase 16

- Un caso particular de la proposición anterior, ítem (ii), da el importante criterio para saber cuando -1 es residuo cuadrático módulo p:
- Proposición: Si p es primo impar, se tiene:
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- Demostración: Aplicamos (ii) de la proposición previa al caso a = -1:
- $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Como p > 2 y ambos valores pertenecen a {-1 , 1}
- de la congruencia deducimos igualdad: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
- Corolario: Sea p primo impar. Entonces se tiene:
- -1 es residuo cuadrático módulo p $\Leftrightarrow$ $p \equiv 1 \pmod{4}$
- Demostración: Sale de la igualdad anterior: Por un lado que -1 sea un residuo cuadrático módulo p equivale a que $\left(\frac{-1}{p}\right) = 1$. Por otro lado, $(-1)^{\frac{p-1}{2}}$ es igual a 1 $\Leftrightarrow$ el exponente (p-1)/2 es par, que equivale a: $\frac{p-1}{2} \equiv 0 \pmod{2}$ $\Leftrightarrow$ $p - 1 \equiv 0 \pmod{4}$ $\Leftrightarrow$ $p \equiv 1 \pmod{4}$.



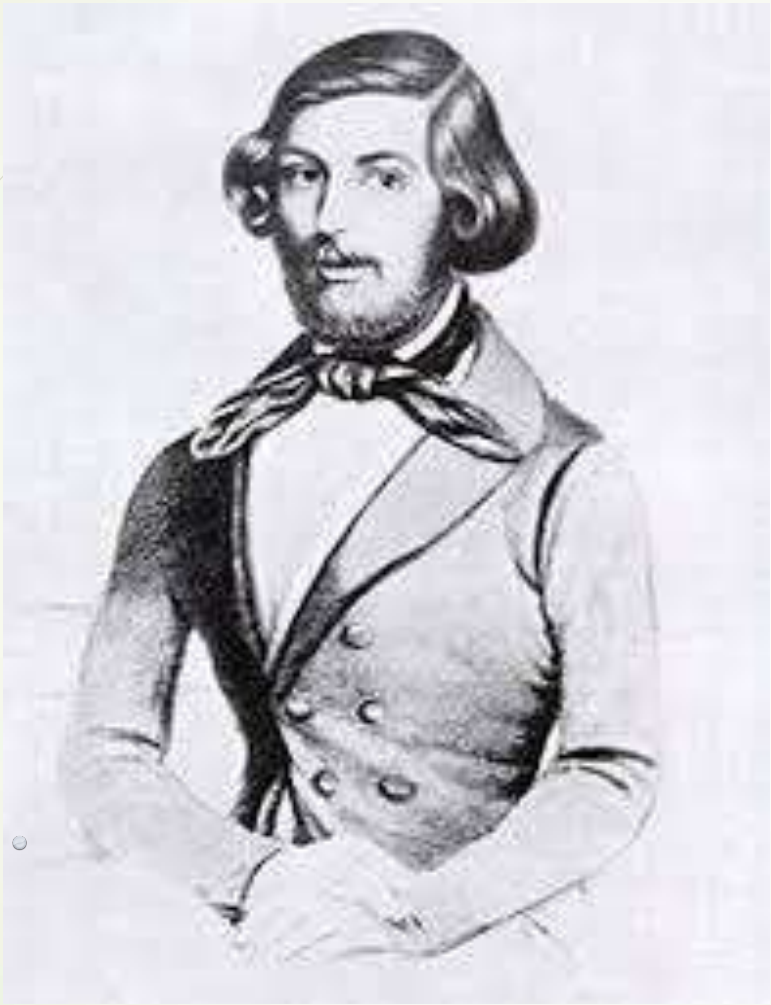
A.-M. Legendre

- Lema de Eisenstein: Sean p y q primos impares distintos. Sea [x] la función parte entera, es decir: para $x \in \mathbb{R}$, [x] es el mayor entero z con $z \leqq x$. Entonces se tiene que:
- $\left(\frac{q}{p}\right) = (-1)^{\sum_u \left[\frac{qu}{p}\right]}$, donde u recorre los números pares con $2 \leqq u \leqq p-1$.
- Demostración: Para u par con $2 \leqq u \leqq p-1$, sea r(u) = resto de dividir q·u por p. Es decir: $r(u) \equiv q \cdot u \pmod{p}$, con $0 < r(u) < p$ (pues no puede dar 0).
- Considero ahora los números $(-1)^{r(u)} \cdot r(u)$, y a cada uno de ellos le asocio el representante de su clase residual módulo p en el intervalo $0 < x < p$:
- $$(-1)^{r(u)} \cdot r(u) \equiv s(u) \pmod{p}, \quad \text{con } 0 < s(u) < p.$$
- Todos los s(u) son pares, pues si r(u) es par ⇨ s(u) = r(u), y si r(u) es impar ⇨
- $s(u) \equiv -r(u) \pmod{p}$ ⇨ s(u) = -r(u) + p , que es par.

- Además, todos los $s(u)$ son distintos, pues si fuera:
- $s(u) = s(t) \Rightarrow (-1)^{r(u)} \cdot r(u) \equiv (-1)^{r(t)} \cdot r(t) \pmod{p} \Rightarrow$
- $(-1)^{r(u)} \cdot q \cdot u \equiv (-1)^{r(t)} \cdot q \cdot t \pmod{p}$, y por la propiedad cancelativa (la aplicamos pues p es coprimo con q) $\Rightarrow u \equiv \pm t \pmod{p}$.
- Pero $u \equiv -t \pmod{p}$ no puede ocurrir, pues si no sería: $u = -t + p$ (hemos utilizado el hecho de u y t están en el intervalo [1, p-1]) contradiciendo el hecho de que u y t son ambos pares.
- Con lo cual tenemos que: $s(u) = s(t) \Rightarrow u \equiv t \pmod{p} \Rightarrow u = t$. Es decir, que todos los $s(u)$ son distintos.
- Por lo tanto, los $s(u)$ son elementos del intervalo [1, p-1], son todos pares, todos distintos, y hay (p-1)/2 de ellos (tantos como u pares en este intervalo)

- Con lo cual concluimos que los s(u) son una permutación de 2, 4, … , p-1 (es decir, de los u pares del intervalo [1, p-1]). Por lo tanto, si considero el producto de todos ellos, se tiene:
- $s(2) \cdot s(4) \cdot \ldots \cdot s(p-1) = 2 \cdot 4 \cdot \ldots \cdot (p-1) \Rightarrow$
- $(-1)^{r(2)} \cdot r(2) \cdot (-1)^{r(4)} \cdot r(4) \cdot \ldots \cdot (-1)^{r(p-1)} \cdot r(p-1) \equiv 2 \cdot 4 \cdot \ldots \cdot (p-1) \pmod{p} \Rightarrow$
- $(-1)^{r(2)} \cdot 2 \cdot q \cdot (-1)^{r(4)} \cdot 4 \cdot q \cdot \ldots \cdot (-1)^{r(p-1)} \cdot (p-1) \cdot q \equiv 2 \cdot 4 \cdot \ldots \cdot (p-1) \pmod{p}$
- Aplicamos la propiedad cancelativa:
- $(-1)^{r(2)+r(4)+\ldots r(p-1)} \cdot q^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow (-1)^{r(2)+r(4)+\ldots r(p-1)} \equiv q^{(p-1)/2} \pmod{p}$
- Por otro lado, al dividir q·u por p, el cociente es $\left[\frac{qu}{p}\right]$ y el resto es r(u), de donde: $q \cdot u = p \cdot \left[\frac{qu}{p}\right] + r(u)$. Como q · u es par y p es impar , vemos de aquí que:
- $\left[\frac{qu}{p}\right]$ y r(u) tienen la misma paridad. Por lo tanto, la fórmula anterior equivale a:

- $q^{(p-1)/2} \equiv (-1)^{\sum_u \left[\frac{qu}{p}\right]} \pmod{p}$, con u par con $2 \leqq u \leqq p-1$.
- De aquí, combinando con el criterio de Euler, tenemos:
- $\left(\frac{q}{p}\right) \equiv (-1)^{\sum_u \left[\frac{qu}{p}\right]} \pmod{p}$. Como ambos miembros valen 1 o -1, de la congruencia módulo p se deduce la igualdad:
- $\left(\frac{q}{p}\right) = (-1)^{\sum_u \left[\frac{qu}{p}\right]}$.



F. Eisenstein

- ## Teorema (Ley de Reciprocidad Cuadrática):
- Sean p y q primos impares distintos. Entonces se tiene:
- $$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$