Clase 19

- Ejemplo de Aplicación: Gracias a la ley de Reciprocidad Cuadrática, podemos determinar si 3 es o no residuo cuadrático módulo p (recordar que la respuesta a esta pregunta la da el símbolo de Legendre $\left(\frac{3}{p}\right)$) para un primo p impar dado p ≠ 3. Aplicando el Corolario anterior, dividimos en dos casos:
- (1) p ≡ 1 (mod 4): En este caso tenemos que
- $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 \ \ si \ \ p \ \equiv \ 1 \ (mod\ 3) \\ -1 \ \ si\ p \ \equiv 2 \ (mod\ 3) \end{cases}$
- (pues es evidente que 1 es residuo cuadrático módulo 3 y 2 no lo es).

- (2) En cambio si p ≡ 3 (mod 4), como 3 también es congruente con 3 módulo 4, el corolario dice que
- $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} -1 \ \ si \ \ p \ \equiv \ 1 \ (mod\ 3) \\ \ \ 1 \ \ si\ p \ \equiv 2 \ \ (mod\ 3) \end{cases}$
- Juntando la información de los dos casos, concluimos que $\left(\frac{3}{p}\right)$ = 1 sí y sólo sí está en los casos siguientes:
- p es congruente con 1 módulo 4 y con 1 módulo 3, o p es congruente con 3 módulo 4 y con 2 módulo 3. Resolviendo estos sistemas de dos congruencias, esto equivale a: p ≡ 1 (mod 12) o p ≡ 11≡ -1 (mod 12).
- Por lo tanto, el caso complementario es: $\left(\frac{3}{p}\right)$ = - 1 ⇔ p ≡ 5 o 7 (mod 12).

- Por lo tanto, por ejemplo tenemos que:
- $\left(\frac{3}{11}\right) = 1$ porque $11 \equiv -1 \pmod{12}$
- $\left(\frac{3}{13}\right) = 1$ porque $13 \equiv 1 \pmod{12}$
- $\left(\frac{3}{17}\right) = -1$ porque $17 \equiv 5 \pmod{12}$
- $\left(\frac{3}{7}\right) = -1$ porque $7 \equiv 7 \pmod{12}$

- Lema de Gauss: Sea p un primo impar y a un entero no divisible por p.
- Sea n la cantidad de enteros del conjunto: S = {a, 2·a, ….. $\left(\frac{p-1}{2}\right)\cdot a\}$
- tales que al dividirlos por p se obtiene un resto mayor que p/2.
- Entonces: $\left(\frac{a}{p}\right)$ = $(-1)^n$
- Demostración: Sean a_1, a_2, …., a_n los elementos de S tales que al dividirlos por p el resto es mayor que p/2. Sean b_1, b_2,……,b_m los otros elementos de S, de modo que: n + m = (p-1)/2.
- Llamemos a'_j (y b'_j) a los restos correspondientes a dividir los a_j por p (los b_j , respectivamente). Se tiene por lo tanto que:

- $\forall\, j \in \{1, 2, \dots, n\}$, $a'_j \equiv a_j \pmod p$, con $\frac{p+1}{2} \leqq a'_j < p$ (#)
- $\forall\, j \in \{1, 2, \dots, m\}$, $b'_j \equiv b_j \pmod p$, con $0 \leqq b'_j \leqq \frac{p-1}{2}$
- Sea $T = \{p - a'_j \;:\; 1 \leqq j \leqq n\} \cup \{b'_j \;:\; 1 \leqq j \leqq m\}$
- Probemos primero que $T = \{1, 2, \dots, (p-1)/2\}$.
- Sabemos que $T \subseteqq \{1, 2, \dots, (p-1)/2\}$, esto es trivial para los elementos b'_j si recordamos que ningún elemento de S es divisible por p (pues son de la forma $a \cdot k$ con a no divisible por p y $0 < k \leqq (p-1)/2$) y por lo tanto ningún resto puede ser 0, y para los elementos de la forma $p - a'_j$ es consecuencia de la desigualdad (#).
- También sabemos que $n + m = (p-1)/2$, con lo cual para establecer la igualdad de conjuntos basta con probar que los elementos en la definición de T son todos diferentes.

- Si $u, v \in \{1, 2, \ldots\ldots, (p-1)/2\}$ y $u \cdot a \equiv v \cdot a \pmod{p} \Rightarrow u \equiv v \pmod{p} \Rightarrow u = v$.
- Luego los n valores de a'_j ,y por lo tanto los n valores de $p - a'_j$, son todos diferentes, y también los m valores de b'_j son todos diferentes.
- Supongamos ahora, razonando por reducción al absurdo que existe $k \in [1, n]$ y $h \in [1,m]$ tales que $p - a'_k = b'_h$. Esto implica que existen u y v en $\{1, 2, \ldots\ldots, (p-1)/2\}$ tales que $p - u \cdot a \equiv v \cdot a \pmod{p}$. De aquí se sigue que:
- $(u+v) \cdot a \equiv 0 \pmod{p}$ y por lo tanto, como p no divide a a, por el Lema Fundamental de la Aritmética se tiene que p divide a u+v. Como $2 \leqq u+v \leqq p-1$, esto nos da una contradicción.
- Queda probado que los $n+m=(p-1)/2$ elementos en la definición de T son todos diferentes, de donde concluimos que $T = \{1, 2, \ldots, (p-1)/2\}$.

- A partir de esta igualdad, multiplicando todos los elementos de este conjunto obtenemos:
- $\left(\frac{p-1}{2}\right)! \equiv$ (p-a'$_1$) · (p-a'$_2$) · …… · (p-a'$_n$) · b'$_1$ · b'$_2$ · ……· b'$_m$ $\equiv$
- $\equiv$ $(-1)^n$ · a'$_1$ · ……· a'$_n$ · b'$_1$ · ……· b'$_m$ $\equiv$ $(-1)^n$ · a_1 · …..· a_n · b_1 · …..· b_m $\equiv$
- $\equiv$ $(-1)^n$ · a · (2·a)· …..·($(\frac{p-1}{2})$ · a) $\equiv (-1)^n \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!$ (mod p) ⇨
- Como p no divide a $\left(\frac{p-1}{2}\right)!$ ⇨ $1 \equiv (-1)^n \cdot a^{\frac{p-1}{2}}$ (mod p) ⇨
- $(-1)^n \equiv a^{\frac{p-1}{2}}$ (mod p) . Combinando con el criterio de Euler:
- $\left(\frac{a}{p}\right) \equiv (-1)^n$ (mod p) ⇨ $\left(\frac{a}{p}\right) = (-1)^n$.

Clase 20

- Teorema: Sea p un primo impar. Entonces:
- $\left(\frac{2}{p}\right) = \begin{cases} 1 \;\; si \;\; p \equiv \;\; 1 \; o \; 7 \;\; (mod \; 8) \\ -1 \;\; si \;\; p \equiv 3 \; o \; 5 \; (mod \; 8) \end{cases}$
- Demostración: Consideramos el conjunto S como en el lema de Gauss para el caso a = 2:
- S = {2, 4, ……, p-1}
- Dividamos la prueba en dos casos:
- (I) p ≡ 1 (mod 4): es fácil determinar quienes son los elementos de S tales que al dividirlos por p se obtiene un resto mayor que p/2, pues como ahora los elementos de S son todos menores que p, ellos mismos son iguales a los respectivos restos, luego son: $\frac{p-1}{2} + 2$, $\frac{p-1}{2} + 4$, …., $\frac{p-1}{2} + 2 \cdot (\frac{p-1}{4})$ = p -1.
- Aquí hemos utilizado que p ≡ 1 (mod 4) ⇨ $\frac{p-1}{2}$ es par ⇨ $\frac{p-1}{2} + 2$ es el menor número par mayor que p/2.

- Como el primer valor en esta lista es $\frac{p-1}{2} + 2$ y el último es $\frac{p-1}{2} + 2 \cdot (\frac{p-1}{4})$, y todos estos números son pares, vemos que en total la cantidad de elementos de S con la propiedad de que al dividirlos por p se obtiene un resto mayor que p/2 es n = (p-1)/4. Aplicando el Lema de Gauss, concluimos que si p ≡ 1 (mod 4) ⇨ $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$.
- Ahora bien, los primos p ≡ 1 (mod 4) caen en dos clases módulo 8, pueden cumplir p ≡ 1 (mod 8) o p ≡ 5 (mod 8) . En el primer caso, $\frac{p-1}{4}$ es par, y en el segundo caso es impar. Por lo tanto concluimos que:
- $\left(\frac{2}{p}\right) = \begin{cases} 1 \ \ si \ \ p \equiv 1 \ \ (mod\ 8) \\ -1 \ \ si \ \ p \equiv \ \ 5\ (mod\ 8) \end{cases}$

- (II) Veamos ahora el caso p ≡ 3 (mod 4). Ahora, los elementos de S tales que el resto de la división por p es mayor que p/2 son:
- : $\frac{p-1}{2}+1$, $\frac{p-1}{2}$ + 3, ..., $\frac{p-1}{2}$ + (2 · ($\frac{p+1}{4}$)-1) = p - 1
- Aquí hemos utilizado que en este caso $\frac{p-1}{2}$ es impar, luego el menor número par mayor que p/2 es $\frac{p-1}{2}+1.$ La cantidad de elementos de este conjunto es por lo tanto la cantidad de números impares en {1,3, ... 2 · ($\frac{p+1}{4}$)-1}, que es igual a la cantidad de números pares en {2,4, ... ,2 · ($\frac{p+1}{4}$)}, que es $\frac{p+1}{4}$.
- Luego concluimos que en este caso se tiene n = $\frac{p+1}{4}$ con lo cual el Lema de Gauss da: Si p ≡ 3 (mod 4) ⇨ $\left(\frac{2}{p}\right)$ = $(-1)^{\frac{p+1}{4}}$. Como en el caso anterior, separamos en dos casos: p ≡ 3 (mod 8) y p ≡ 7 (mod 8) y concluimos que:

- $\left(\frac{2}{p}\right) = \begin{cases} 1 \;\; si \;\; p \equiv 7 \;\; (mod\ 8) \\ -1 \;\; si \;\; p \equiv \;\; 3\ (mod\ 8) \end{cases}$

- Símbolo de Jacobi: Definición: Sean n > 1 entero impar y a ∊ $\mathbb{Z}$.
- Si n = ${p_1}^{e_1} \cdot {p_2}^{e_2} \cdot \ldots\ldots\ldots {p_r}^{e_r}$ definimos el Símbolo de Jacobi $\left(\frac{a}{n}\right)$ como:
- $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \left(\frac{a}{p_2}\right)^{e_2} \cdot \ \ldots \ldots . \cdot \left(\frac{a}{p_r}\right)^{e_r}$, donde en la expresión anterior los factores a la derecha son símbolos de Legendre.
- Es evidente que el Símbolo de Jacobi generaliza al de Legendre.

- Observación Importante: Si n es compuesto y mcd(a,n)=1, el valor del símbolo de Jacobi $\left(\frac{a}{n}\right)$ NO DETERMINA DE MODO DIRECTO si a es o no residuo cuadrático módulo n. Por ejemplo, si n =15 y a = 2 se tiene:
- $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$, pero como no hay solución para la congruencia $x^2 \equiv 2 \pmod 3$, no puede haber solución para $x^2 \equiv 2 \pmod{15}$, luego 2 no es residuo cuadrático módulo 15.
- Propiedades Básicas: Sean b,d enteros positivos impares mayores que 1, y a, c ∈ ℤ. Se tiene:
- (a) Si a ≡ c (mod b) ⇨ $\left(\frac{a}{b}\right) = \left(\frac{c}{b}\right)$
- (b) $\left(\frac{a \cdot c}{b}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{c}{b}\right)$
- (c) $\left(\frac{a}{b \cdot d}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{d}\right)$
- Demostración: (a) y (b) se deducen de que el símbolo de Legendre tiene estas propiedades. (c) sale directamente de la definición de símbolo de Jacobi.

- Propiedades de Reciprocidad: Si a y b son enteros positivos mayores que 1, impares y coprimos:
- (a) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$
- (b) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$
- (c) $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) \cdot (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$
- Observación: En el caso en que b es primo la propiedad (b) equivale a la fórmula que ya probamos para el símbolo de Legendre $\left(\frac{2}{b}\right)$.
- Para probar este resultado, necesitamos antes probar 3 lemas.

- Lema 1: Si a, b son enteros impares: $\frac{a\cdot b-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$
- Demostración: Como a-1 y b-1 son ambos pares ⇨ $(a-1)\cdot(b-1) \equiv 0 \pmod 4$,
- Luego: $a\cdot b - a - b + 1 \equiv 0 \pmod 4$ ⇨ $a\cdot b + 1 \equiv a + b \pmod 4$ ⇨
- $a \cdot b - 1 \equiv (a-1) + (b-1) \pmod 4$ ⇨ $\frac{a\cdot b-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$
- Lema 2: Si a, b enteros impares:
- $\frac{a^2\cdot b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2$ (&)
- Demostración: Como $a^2 - 1 \equiv 0 \pmod 4$ y $b^2 - 1 \equiv 0 \pmod 4$ ⇨
- $(a^2 - 1) \cdot (b^2 - 1) \equiv 0 \pmod{16}$ ⇨ $a^2 \cdot b^2 - a^2 - b^2 + 1 \equiv 0 \pmod{16}$ ⇨
- $a^2 \cdot b^2 - 1 \equiv a^2 + b^2 - 2 \equiv (a^2 - 1) + (b^2 - 1) \pmod{16}$. De aquí se obtiene (&) dividiendo por 8 ambos miembros. Nótese que todos los términos de la fórmula (&) son enteros pues para todo w impar se tiene $w^2 \equiv 1 \pmod 8$, con lo cual 8 divide a $w^2 - 1$.

- Lema 3: Si a, b, c impares y mayores que 1, suponiendo que:
- $\left(\frac{a}{c}\right) \cdot \left(\frac{c}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{c-1}{2}}$ y que: $\left(\frac{b}{c}\right) \cdot \left(\frac{c}{b}\right) = (-1)^{\frac{b-1}{2} \cdot \frac{c-1}{2}}$, entonces vale:
- $\left(\frac{a \cdot b}{c}\right) \cdot \left(\frac{c}{a \cdot b}\right) = (-1)^{\frac{a \cdot b-1}{2} \cdot \frac{c-1}{2}}$
- Demostración:
- $\left(\frac{a \cdot b}{c}\right) \cdot \left(\frac{c}{a \cdot b}\right) = \left(\frac{a}{c}\right) \cdot \left(\frac{b}{c}\right) \cdot \left(\frac{c}{a}\right) \cdot \left(\frac{c}{b}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{c-1}{2} + \frac{b-1}{2} \cdot \frac{c-1}{2}} = (-1)^{\frac{c-1}{2} \cdot \left(\frac{a-1}{2} + \frac{b-1}{2}\right)}$,
- Y por el lema 1, esto es igual a: $(-1)^{\frac{c-1}{2} \cdot \frac{a \cdot b-1}{2}}$