Clase 13

- Definición: Si a es un entero con mcd(a,m) =1 y el orden de a módulo m es igual a $\varphi(m)$ decimos que a es raíz primitiva módulo m.
- Advertencia: No es cierto que para cualquier módulo m existen raíces primitivas. Por ejemplo si m=8 no hay raíces primitivas: toda clase a inversible módulo 8 cumple $a^2 \equiv 1 \ (módulo\ 8)$ y por lo tanto tiene orden 1 o 2, con lo cual no existen elementos de orden $\varphi(8) = 4$.
- Teorema: Sea m un módulo y sea a una raíz primitiva módulo m. Entonces los elementos del conjunto:
- $S = \{ a, a^2, \ldots . a^{\varphi(m)} \}$ recorren todas las clases residuales inversibles módulo m.

- Demostración: Como mcd(a,m)=1, también $mcd(a^i, m) = 1$, para todo $i = 1,2,\ldots,\varphi(m)$, con lo cual todos los elementos de S corresponden a clases inversibles módulo m. Como la cantidad de clases inversibles módulo m es $\varphi(m)$, basta con probar que todos estos elementos caen en clases residuales diferentes. Por hipótesis, el orden de a módulo m es $\varphi(m)$, por lo tanto si suponemos que $a^i \equiv a^j \ (módulo\ m)$ por el corolario previo concluimos que $i \equiv j \ (módulo\ \varphi(m))$, con lo cual i = j (pues ambos valores están en el intervalo $[1, \varphi(m)]$). Esto prueba que los elementos de S caen todos en clases residuales diferentes, ergo recorren todas las $\varphi(m)$ clases residuales inversibles módulo m.

- Probemos ahora la afirmación recíproca:
- Proposición: Sea m un módulo y a coprimo con m tal que: los elementos de
- $S = \{ a, a^2, \ldots . a^{\varphi(m)} \}$ recorren todas las clases residuales inversibles módulo m. Entonces a es raíz primitiva módulo m.
- Demostración: Como S tiene $\varphi(m)$ elementos y éstos recorren todas las $\varphi(m)$ clases inversibles módulo m, está claro que todos los elementos de S caen en clases residuales diferentes. Como por el Teorema de Euler sabemos que $a^{\varphi(m)} \equiv 1\ (módulo\ m)$ concluimos que este es el único elemento de S en la clase residual del 1, y esto equivale a decir que $\varphi(m)$ es el mínimo exponente positivo e tal que $a^e \equiv 1\ (módulo\ m)$, es decir, que el orden de a módulo m es $\varphi(m)$, con lo cual a es raíz primitiva módulo m.

- Observación: la conclusión de los dos resultados previos es que la existencia de una raíz primitiva módulo m es equivalente a la existencia de una clase inversible módulo m cuyas potencias generan todo $(\mathbb{Z}/m\mathbb{Z})*$.

- Más adelante estudiaremos para qué módulos existen raíces primitivas. Probaremos muchos casos de la siguiente equivalencia:

- Existen raíces primitivas módulo m $\Leftrightarrow$ $m = 1, 2, 4, p^r \ o \ 2 \cdot p^r$, con p primo impar.

- Veremos a continuación que para un módulo primo p siempre existen raíces primitivas módulo p. Recordad que φ(n) denota la función de Euler que cuenta la cantidad de enteros positivos menores o iguales que n que son coprimos con n.
- Lema: Si n ≧ 1, se tiene:
- n = $\sum_{d|n} \varphi(d)$
- Demostración: Consideremos $\mathbb{Z}/n\mathbb{Z}$, el conjunto de todas las clases residuales módulo n, el cual tiene n elementos. Particionemos este conjunto de acuerdo al valor de mcd(x,n), para x un representante de cada clase residual, el cual cogemos en el intervalo 1 ≦ x ≦ n.

- Nótese que cualquiera sea x, se tiene que mcd(x,n) es un divisor de n, luego si consideramos para cada a que divide a n el conjunto:
- R_a = {clase residual $\bar{x} \in \mathbb{Z}/ n\mathbb{Z}$ tal que mcd(x,n) = a}
- Se tiene que $\mathbb{Z}/n\mathbb{Z}$ queda particionado en estos conjuntos R_a donde a recorre los divisores de n. Por lo tanto se tiene que:
- $\mathbb{Z}/n\mathbb{Z} = \coprod_{a|n} R_a$ (el símbolo $\coprod$ denota unión disjunta de conjuntos).
- Por lo tanto n, el cardinal de $\mathbb{Z}/n\mathbb{Z}$, es igual a la suma de los cardinales de los conjuntos R_a cuando a recorre los divisores de n. Nos queda por determinar el cardinal de estos conjuntos R_a .

- Si a | n y x ∈ {1, 2, ….., n} cumple x ∈ R_a ⟹ mcd(x,n) = a con lo cual podemos escribir x = i · a, n = a' · a con 0 < i ≦ a' (que equivale a 0 < x ≦ n) y mcd(i, a') = 1 (esta condición equivale a mcd(x, n) = a).
- Por lo tanto hay tantos elementos en R_a como enteros i tales que:
- 0 < i ≦ a' y mcd(i, a') = 1. Ergo, hay $\varphi(a')$ elementos en R_a , donde a' = n/a.
- Luego:
- n = #(ℤ/nℤ) = $\sum_{a|n} \# R_a = \sum_{a|n} \varphi(\frac{n}{a})$
- Esta sumatoria es sobre todos los divisores a de n. Observamos que cuando a recorre todos los divisores de n, n/a también recorre todos los divisores de n, luego concluimos que: n = $\sum_{b|n} \varphi(b)$.
- Q. E. D.

- Para probar el siguiente lema, observemos que el Pequeño Teorema de Fermat establece que si p es primo la congruencia de grado p-1:
- $$x^{p-1} \equiv 1 \pmod{p}$$
- posee p-1 soluciones (todas las clases módulo p diferentes de la del 0).
- Recordemos también que gracias al Teorema de Lagrange sabemos que si F(x) es un polinomio a coeficientes enteros de grado $k > 0$ (y tal que su reducción módulo p también es de grado k) la congruencia:
- $$F(x) \equiv 0 \pmod{p}$$
- Posee como máximo k soluciones.

- Lema: Si p es primo y d > 0 es un divisor de p-1, la congruencia:
- $$x^d \equiv 1 \pmod{p}$$
- Tiene exactamente d soluciones.
- Demostración: Para empezar, sabemos gracias al Teorema de Lagrange que no puede tener más de d soluciones.
- Como p-1 = k · d, se tiene la factorización:
- $x^{p-1} - 1 = (x^d)^k - 1 = (x^d - 1) \cdot Q(x)$ (😋)
- donde Q(x) es un polinomio a coeficientes enteros, de grado p-1-d.
- Como ya mencionamos, sabemos gracias a Fermat que la congruencia
- $X^{p-1} - 1 \equiv 0 \pmod{p}$ posee p-1 soluciones. Por la fórmula (😋), si r es solución de esta congruencia, o bien r es solución de $x^d - 1 \equiv 0 \pmod{p}$ o bien lo es de $Q(x) \equiv 0 \pmod{p}$. Aquí hemos utilizado el Lema Fundamental de la Aritmética igual que como hicimos en el Teorema de Lagrange: si p divide a un producto, tiene que dividir a alguno de los factores ⇨ si r es "raíz módulo p" del polinomio producto, lo será también del alguno de los polinomios que se multiplican.

- Por lo tanto, de las p-1 soluciones de $x^{p-1} - 1 \equiv 0 \pmod{p}$, todas las que no sean solución de $x^d - 1 \equiv 0 \pmod{p}$ tienen que ser solución de la congruencia de grado p-1-d: $Q(x) \equiv 0 \pmod{p}$, entonces tenemos por Lagrange que hay un máximo de p-1-d de ellas.
- Tenemos por lo tanto un conjunto de p-1 clases modulo p de las cuales un máximo de p-1-d NO resuelven la congruencia $x^d - 1 \equiv 0 \pmod{p}$, y por lo tanto habrá un mínimo de d de estas clases módulo p que sí resuelven esta congruencia.
- Como mencionamos al comenzar, sabemos por Lagrange que no puede haber más de d soluciones, ergo el número de soluciones es exactamente igual a d.
- Q. E. D.

Clase 14

- Teorema: Si p es primo y d > 0 es divisor de p-1, de las d clases módulo p que son solución de:
- $x^d \equiv 1 \pmod{p}$
- hay exactamente $\varphi(d)$ de ellas que tienen orden d módulo p.
- En particular, hay $\varphi(p-1)$ clases inversibles módulo p que tienen orden p-1 módulo p, es decir, que son raíces primitivas módulo p.
- Observación: El teorema implica en particular que existen raíces primitivas módulo p para todo p primo.

- Demostración: Sea r un elemento de una clase inversible módulo p, de orden d. En particular, es solución de la congruencia $x^d - 1 \equiv 0 \pmod{p}$.
- Luego, la cantidad de clases que son solución de $x^d - 1 \equiv 0 \pmod{p}$ y tienen orden d es igual a la cantidad de clases inversibles módulo p de orden d. Para cada d divisor de p-1, llamemos $\psi(d)$ a esta cantidad.
- Sabemos que todo elemento en {1, 2,…., p-1} tiene por orden módulo p a un divisor de p-1, de donde:
- $\sum_{d \mid p-1} \psi(d) = p - 1$
- (es decir: la igualdad anterior sale de particionar el conjunto de las clases inversibles módulo p en subconjuntos de acuerdo al orden módulo p de sus elementos).

- Por otro lado, vimos en un lema previo que se tiene: $\sum_{d \mid p-1} \varphi(d) = p - 1$.
- Por lo tanto, si pudiéramos probar que, para todo d | p-1, se tiene: $\psi(d) \leqq \varphi(d)$, se tendría:
- p-1 = $\sum_{d \mid p-1} \psi(d) \leqq \sum_{d \mid p-1} \varphi(d)$= p-1 y por lo tanto que para todo d | p-1 vale la igualdad $\psi(d) = \varphi(d)$. Es decir: la cantidad de soluciones de $x^d - 1 \equiv 0 \pmod p$ que tienen orden d es $\varphi(d)$, que es lo que queremos probar.
- Por lo tanto, sólo falta probar que se tiene: $\psi(d) \leqq \varphi(d)$, para todo d | p-1.
- Sea d un divisor de p-1 y sea f ∈ {1, 2, …., p-1} de orden d módulo p. Si no existiera un tal f: $\psi(d) = 0 \leqq \varphi(d)$ y se acaba el argumento.
- Consideremos los d números: $f_h = f^h$, con exponente h ∈ {0, 1, …., d-1}.

- $f^d \equiv 1 \pmod{p} \Longrightarrow f^{hd} \equiv 1 \pmod{p} \Longrightarrow$ los d números f_h , con h=0, 1,.., d-1 son todos solución de $x^d \equiv 1 \pmod{p}$. Además son dos a dos no congruentes módulo p pues si:
- $h \geqq h'$ y $f_h \equiv f_{h'} \pmod{p} \Longrightarrow f^h \equiv f^{h'} \pmod{p} \Longrightarrow f^{h-h'} \equiv 1 \pmod{p}$ y como $0 \leqq h - h' \leqq d - 1$ y f tiene orden d concluímos que $h = h'$.
- Luego, como la congruencia $x^d \equiv 1 \pmod{p}$ tiene d soluciones módulo p, vemos que los números f_h recorren (sin repetir) todas las clases módulo p que son solución de esta congruencia.

- En particular, toda clase de orden d está representada por algún f_h (*).
- Además, es fácil ver que si f tiene orden d módulo p, entonces f_h tiene orden menor o igual que d/mcd(d,h) módulo p. De aquí se deduce que si f_h también tiene orden d, entonces mcd(d,h) = 1. Junto con (*), concluimos que la cantidad de clases módulo p de orden d es como mucho la cantidad de clases coprimas con d, es decir, que:
- $\psi(d) \leqq \varphi(d)$, para todo $d \mid p-1$. Como ya mencionamos, esto basta para acabar la demostración del teorema.

- RAÍCES PRIMITIVAS:

- El teorema previo implica la existencia de raíces primitivas módulo p para todo p primo.
- Si m=4, $\varphi(4)=2$ y 3 tiene orden 2 módulo 4, luego 3 es raíz primitiva módulo 4.
- Si m=8, $\varphi(8)=4$ pero las 4 clases inversibles módulo 8 tienen orden 1 o 2 pues:
- $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$ (módulo 8), luego no existen raíces primitivas módulo 8.
- Si $r \geqq 3$ veamos que no existen raíces primitivas módulo 2^r utilizando el siguiente resultado:

- Lema: Si la ecuación $x^2 \equiv 1 \pmod{m}$ posee más de dos soluciones, entonces no existen raíces primitivas módulo m.
- Demostración: Razonemos por contradicción: supongamos que existen raíces primitivas módulo m y sea a una tal raíz. Esto significa que el orden de a módulo m es $\varphi(m)$, y vimos que en este caso se tiene que:
- $a, a^2, \ldots, a^{\varphi(m)}$ recorren todas las $\varphi(m)$ clases inversibles módulo m.
- Dado w tal que $w^2 \equiv 1 \pmod{m}$, se tiene por lo tanto un $r \in \{1, 2, \ldots, \varphi(m)\}$ tal que $w \equiv a^r \pmod{m}$. De aquí, elevando al cuadrado se obtiene:
- $a^{2r} \equiv 1 \pmod{m}$, y como a tiene orden $\varphi(m) \Longrightarrow \varphi(m) \mid 2r$. Teniendo en cuenta que $r \in \{1, 2, \ldots, \varphi(m)\}$ es evidente que esto sólo puede ocurrir si $r= \varphi(m)$ o $r= \varphi(m)/2$ (este último caso si $\varphi(m)$ es par, que equivale a $m > 2$).
- Por lo tanto un w que es solución de $x^2 \equiv 1 \pmod{m}$ tiene que cumplir $w \equiv a^r \pmod{m}$ para $r = \varphi(m)$ o $\varphi(m)/2$, con lo cual hay sólo (como máximo) dos soluciones de esta congruencia cuadrática, contradiciendo la hipótesis del lema.

- Corolario 1: Si $r \geqq 3$ y $m = 2^r$ no existen raíces primitivas módulo m.
- Demostración: Basándonos en el lema previo, basta con probar que hay más de dos soluciones para $x^2 \equiv 1 \pmod{2^r}$. Por un lado, tenemos las soluciones triviales 1 y $2^r - 1$. Por otro lado, como:
- $X^2 - 1 \equiv 0 \pmod{2^r} \iff (x + 1)(x-1) \equiv 0 \pmod{2^r}$.
- Para cualquier z impar que se escoja, como $2 \mid z + 1$, bastará con que se tenga $2^{r-1} \mid z - 1$ para que nos sirva. Por lo tanto, podemos coger por ejemplo: $z = 2^{r-1} + 1$ como solución de la congruencia cuadrática. Es fácil ver que para todo $r \geqq 3$ este z cumple $1 < z < 2^r - 1$, con lo cual concluimos que hay al menos 3 soluciones de la congruencia $x^2 \equiv 1 \pmod{2^r}$.

- Corolario 2: Si p y q son primos impares diferentes y m= p·q, no existen raíces primitivas módulo m.
- Demostración: Aplicando nuevamente el lema, basta con ver que hay más de dos soluciones de $x^2 \equiv 1 \pmod{m}$. Esta congruencia equivale a:
- $(x + 1)(x-1) \equiv 0 \pmod{p \cdot q} \Leftrightarrow (x+1)(x-1) \equiv 0 \pmod{p}$ y $(x+1)(x-1) \equiv 0 \pmod{q}$, que equivale a:
- $x \equiv \pm 1 \pmod{p}$ y $x \equiv \pm 1 \pmod{q}$ (donde los dos signos ± son independientes uno del otro). Cogiendo ambos signos en cada congruencia obtenemos en total 4 sistemas de congruencias lineales, y cada uno de ellos posee (Teorema Chino de los Residuos) una solución única módulo p·q. Por lo tanto vemos que hay al menos 4 soluciones de $x^2 \equiv 1 \pmod{m}$, de donde por el lema concluimos que no existen raíces primitivas módulo m.

- Ejercicio: Con la ayuda del lema previo, probad que si m es múltiplo de p·q, con p y q primos impares diferentes, o si es múltiplo de 4·p con p primo impar, entonces no existen raíces primitivas módulo m.