Tarea: Relaciones de equivalencia, congruencias con residuos y generadores multiplicativos.

Estimados estudiantes,

Resolver los siguientes ejercicios en el formato adjunto y cargar en la tarea correspondiente.

Ejercicios. Dividimos esta tarea en 3 partes (todas estrechamente ligadas).

Parte 1: Relaciones de equivalencia

Dado un conjunto abstracto X, una relación de equivalencia sobre X es un subconjunto $R \subset X \times X$ tal que

* Es reflexiva: todo $x \in X$ satisface $(x, x) \in R$ * Es simétrica: si $(x, x') \in R$ entonces $(x', x) \in R$ * Es transitiva: si $(x, x') \in R$ y $(x', x'') \in R$ entonces $(x, x'') \in R$

Demuestre que:

Ejercicio: Si X son los enteros muestre que la relación "divide a" no es de equivalencia por "fallar la simetría", formalmente sea R el conjunto de pares (x,x') tales que $x|x'$ (es decir, x divide a x', lo que significa que x es factor de x', en el lenguaje de las ecuaciones $x' = xq$ para cierto cociente q entero). Entonces pruebe que esta R satisface reflexiva y transitiva, pero no siempre simetría.

Ejercicio: Aca nos ponemos geométricos. Resuelva los incisos (a) y (b). Para el primero puede usar que las rectas del plano son paraleleas cuando mantienen la misma distancia en toda su extensión. (a) Tome X como las rectas del plano y defina (r,r') en R si r es paralela a r' y muestre que R es de equivalencia (tambié puede usar la definición de paralelismo por ecuaciones de rectas, es decir cuando las pendientes son iguales). (b) Tome X los triángulos en el plano real, y defina (x,x') en R sii x es congruente como triángulo a x'; lo que significa que hay una correspondencia entre vértices que respeta ángulos y longitudes de lados, entonces pruebe que R es de equivalencia.

Ejercicio: Muestre que la relación "a es congruente a b módulo n" es de euivalencia en los enteros. Formalmente, sea X=enteros, defina (a,b) en R si $n|(a-b)$, muestre que esta relación R es de equivalencia.

Parte 2: Congruencias módulo entero (recuerde que $a =_n b$ significa $n|a-b$ y que sus clases de equivalencia quedan $\bar{a} = \bar{b}$)

En este caso, recordemos que por el algoritmo de división los residuos nos dan los "representantes canónicos" $\bar{0}, ..., \overline{n-1}$ para Z_n, es decir, basta calcular el residuo de an para tener el representante canónico de a, formalmente $\bar{a} = \overline{nq + r} = \bar{r}$ donde el residuo siempre satisface $0rn$. La clase de a denotada por $\bar{a}$ es el conjunto $\{b \in Z : b =_n a\} = \{b : b = nc + a\}$

Ejercicio: Encuentre el representante canónico de $\bar{x}$ en Z_n, cuando $x = 35, n = 8$.

Ejercicio: Encuentre el representante canónico de $\bar{x}$ en Z_n, cuando $x = 230, n =$

59.

Ejercicio: Encuentre el representante canónico de $\bar{x}$ en Z_n, cuando $x = 68, n = 25$.

Parte 2: Generadores del conjunto multiplicativo Z_p^* con p primo.

En este caso, pasar de Z_p a Z_p^* solamente es quitar al cero (neutro de la suma) $\bar{0}$ y nos da $Z_p^* = Z_n - \{\bar{0}\}$, dado que p es primo este conjunto es cerrado multiplicativamente. Adicionalmente siempre tiene un generador g, esto es, un entero tal que todo elemento en Z_p^* es una potencia de la forma $(\bar{g})^n = \overline{g^n}$.

Ejercicio: Encuentre un generador $\bar{g}$ de Z_p, cuando $p = 37$ y halle el exponente e (logaritmo) adecuado para $\overline{300} = \bar{g}^e$

Ejercicio: Encuentre un generador $\bar{g}$ de Z_p, cuando $p = 317$ y halle el exponente e (logaritmo) adecuado para $\overline{2000} = \bar{g}^e$

Ejercicio: Encuentre un generador $\bar{g}$ de Z_p, cuando $p = 53$ y halle el exponente e (logaritmo) adecuado para $\overline{80} = \bar{g}^e$