Prueba 1, Teoría de Números, 2do semestre 2024.

Escriba su NOMBRE en cada una de las hojas que entregue.

Para cada pregunta escriba claramente su respuesta final, sus argumentos y cálculos. Puede usar cualquier resultado mencionado en clases sin necesidad de demostrarlo. Sin embargo debe indicar donde ha sido visto.

1.- (1.2 pts.) Sea $a = 36$ y $b = 10$. Calcule $g = \gcd(a, b)$ y encuentre $\alpha, \beta \in \mathbb{Z}$ tal que $g = a\alpha + b\beta$.

2.- (2 pts.) Sean a y b dos enteros relativamente primos. Sea c cualquier entero.

a) Demuestre que la ecuación $ax + by = c$ siempre tiene alguna solución $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

b) Sea (x_0, y_0) una solución en $\mathbb{Z} \times \mathbb{Z}$ de la ecuación $ax + by = c$. Demuestre que para toda otra solución $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ de la misma ecuación, existe algún $t \in \mathbb{Z}$ tal que

$$x = x_0 + bt, \qquad y = y_0 - at$$

c) Sea (x_0, y_0) como antes. Demuestre la siguiente igualdad de conjuntos

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \text{ tal que } ax + by = c\} = \{(x_0 + bt, y_0 - at) \text{ tal que } t \in \mathbb{Z}\}$$

3.- (2 pts.) Recordar que el conjunto de todos los triples pitagoricos primitivos (a, b, c) con a impar es

$$\left\{ \left(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2} \right) \text{ tal que } 1 \leq t < s \text{ son enteros impares, } \gcd(t, s) = 1 \right\}.$$

Encuentre una descripción del conjunto de todos los triples pitagoricos primitivos (a, b, c) con a impar tal que $c = a + 2$. Justifique su reapuesta.

4.- (0.8 pts.) Sean b, c enteros relativamente primos, e.d. $\gcd(c, d) = 1$.

Demuestre que para todo $a \in \mathbb{Z}$ se tiene que $\gcd(a, b) \cdot \gcd(a, c)$ divide a $\gcd(a, bc)$.

Respuestas

1.- Primero realizamos las siguientes divisiones,

$$36 = 3 \cdot 10 + 6$$

$$10 = 1 \cdot 6 + 4$$

$$6 = 1 \cdot 4 + 2$$

$$4 = 2 \cdot 2 + 0$$

Por un teorema visto en clases, sabemos que $g = \gcd(a, b) = 2$. De estas divisiones también notamos que

$$2 = 6 - 4 = 6 - (10 - 6) = 2 \cdot 6 - 10 = 2 \cdot (36 - 3 \cdot 10) - 10 = 2 \cdot 36 - 7 \cdot 10.$$

Por lo tanto

$$2 = 36\alpha + 10\beta, \quad \text{con } \alpha = 2,\ \beta = -7$$

2.- a) El que a y b son relativamente primos nos dice que $\gcd(a, b) = 1$. Entonces existen enteros α y β tal que $a\alpha + b\beta = 1$.

Sea c cualquier entero. Entonces tenemos $a\alpha c + b\beta c = c$.

Por lo tanto la ecuación $ax + by = c$ tiene solución $(x = \alpha \cdot c,\ y = \beta \cdot c)$ en $\mathbb{Z} \times \mathbb{Z}$.

b) Sea $(x_0, y_0), (x, y) \in \mathbb{Z} \times \mathbb{Z}$ pares de enteros que satisfacen la relación $ax + by = c$. Entonces

$$ax_0 + by_0 = c \quad \text{y} \quad ax + by = c.$$

Por lo tanto $ax + by - ax_0 - by_0 = 0$. Es decir $a(x - x_0) + b(y - y_0) = 0$. Entonces

$$a(x - x_0) = -b(y - y_0).$$

De esta última ecuación es claro que $a|b(y - y_0)$ y $b|a(x - x_0)$. Ya que $\gcd(a, b) = 1$ por hipótesis, podemos usarun teorema visto en clases y concluir

$$b|(x - x_0) \quad \text{y} \quad a|(y - y_0).$$

Digamos $x - x_0 = bt$ y $y - y_0 = at'$ para ciertos enteros t, t'. Finalmente, notamos que

$$a(x - x_0) = -b(y - y_0) \implies abt = -bat' \implies t = -t'.$$

Por lo tanto, hemos probado que existe $t \in \mathbb{Z}$ tal que $x = x_0 + bt$ e $y = y_0 - at$.

c) Por el argumento anterior sabemos que toda solución (x, y) de la ecuación dada es de la forma $x = x_0 + bt$, $y = y_0 - at$ para algún $t \in \mathbb{Z}$. Esto prueba la conteción

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \text{ tal que } ax + by = c\} \subseteq \{(x_0 + bt, y_0 - at) \text{ tal que } t \in \mathbb{Z}\}$$

Por otro lado, si $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ es solución de la ecuación y $t \in \mathbb{Z}$, entonces el par $(x_0 + bt, y_0 - at) \in \mathbb{Z} \times \mathbb{Z}$ y además

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + abt + by_0 - bat = ax_0 + by_0 = c.$$

Por lo tanto $(x_0 + bt, y_0 - at)$ es solución de la ecuación. Esto demuestra que

$$\{(x_0 + bt, y_0 - at) \text{ tal que } t \in \mathbb{Z}\} \subseteq \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \text{ tal que } ax + by = c\}$$

las dos contenciones demuestran lo pedido.

3.- Por lo visto en clases, estamos buscando todos los triples de enteros de la forma

$$\left(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}\right) \text{ tal que } 1 \leq t < s \text{ son enteros impares, } \gcd(t, s) = 1$$

y además satisfacen

$$\frac{s^2 + t^2}{2} = st + 2, \text{ es decir } s^2 + t^2 = 2st + 4. \text{ En otras palabras, } s^2 - 2st + t^2 = 4.$$

Como esto equivale a $(s - t)^2 = 4$, y $t < s$, concluimos $s - t = 2$. Entonces el conjunto pedido es el de los triples

$$\left((2 + t)t, \frac{(2 + t)^2 - t^2}{2}, \frac{(2 + t)^2 + t^2}{2}\right) \text{ tal que } 1 \leq t \text{ es un entero impar}$$

Es decir

$$\left((2 + t)t, 2 + t, 2 + t + t^2\right) \text{ tal que } 1 \leq t \text{ es un entero impar}$$

4.- Sean $g = \gcd(a, b)$ y $h = \gcd(a, c)$. Claramente $g|b$ y $h|c$ implican que $(gh)|(bc)$.

Por otro lado, $g|a$ y $h|a$ implican $a = ga'$ y $a = ha''$ para ciertos $a', a'' \in \mathbb{Z}$.

Notamos además que $\gcd(g, h)$ divide a ambos g y h. Por lo tanto, también divide a ambos b y c. Esto significa que $\gcd(g, h)$ divide a $\gcd(b, c)$ (por resultado visto en clases). Así, $\gcd(g, h)$ divide a $\gcd(b, c) = 1$. Entonces $\gcd(g, h) = 1$.

Ahora bien,

$$a = ga' \text{ y } a = ha'' \implies h|ga'$$

Y como $\gcd(g, h) = 1$, por un resultado visto en clases concluimos $h|a'$. De esta manera tenemos $a' = hr$ para algún $r \in \mathbb{Z}$. Así, $a = ga' = ghr$. Por lo tanto $(gh)|a$.

De $(gh)|a$ y $(gh)|bc$ obtenemos $(gh)|\gcd(a, bc)$ (acá volvemos a usar un resultado visto en clases).