Real Bermúdez Jesús M.

June 8, 2003

1. Ejercicios de las notas de Teoría de Números

Probar que si G es grupo cíclico finito y $g \in G$, cuyo orden es k, entonces $< g >= G \Leftrightarrow (k, o(G)) = 1$.

Demostración

$\Leftarrow$) Supongamos que $o(G) = n$. Sea $g = h^k$ con $1 \leq k < n$ y $(k, n) = 1$. Veamos que $G =< g >$.
Sea $c \in G \Rightarrow$ existe $t \in \mathbb{Z}$ tal que $c = h^t$. Como $(k, n) = 1 \Rightarrow$ existe $r, s \in \mathbb{Z}$ talque $kr + ns = 1 \Rightarrow$

$$c = h^t = h^{krt+nst} = (h^n)^{st} \cdot (h^k)^{rt} = (h^k)^{rt} = g^{rt} \in < g >$$

Asi que $G =< g >$.

$\Rightarrow$) Sea $g \in G$ tal que $G =< g > \Rightarrow$ existe $a \leq k < n$ tal que $g = h^k \in G$.
Además existe $m \in \mathbb{Z}$ tal que $h = g^m$
$\Rightarrow h = g^m = (h^k)^m = h^{km}$
$\Rightarrow h^{km-1} = e$
$\Rightarrow n|(km - 1)$
$\Rightarrow$ existe $r \in \mathbb{Z}$ tal que $nr = km - 1$
$\Rightarrow 1 = n(-r) + km$
$\Rightarrow (n, k) = 1$

q.e.d.

1. Explicar porqué a pesar de que $U_n \subset \mathbb{Z}/n\mathbb{Z}$ se tiene que U_n no es subgrupo de $\mathbb{Z}/n\mathbb{Z}$.

Respuesta

Porque $\mathbb{Z}/n\mathbb{Z}$ no le hereda la operación a U_n, ya que $\mathbb{Z}/n\mathbb{Z}$ es grupo bajo la operación suma $n\mathbb{Z} + n'\mathbb{Z} = (n + n')\mathbb{Z}$ y U_n es grupo abeliano bajo la operación producto $([m], [n]) = [mn]$.

2. Averiguar la identidad de U_n

Solución

Sea $[1] \in U_n$ y $[1] \cdot [a] = [1 \cdot a] = [a] \quad \forall [a] \in U_n$
Por lo tanto [1] es la identidad en U_n.

3. Dado $[m] \in U_n$ ¿Cuál es su inverso en U_n?.

Respuesta

Dado $[a] \in U_n$, encontremos $[a'] \in U_n$ tal que $[a][a'] = [1]$.
Puesto que $(a, n) = 1$ existe $a', n' \in \mathbb{Z}$ tal que $1 = aa' + nn'$, tomando clases módulo n, se tiene:

$$[1] = [aa'] + [nn'] = [aa'] = [a][a']$$

y además $(a', n) = 1$.
Por tanto $[a'] \in U_n$.

2. Ejercicios de la sección 2.7 de Teoría de Números

2. Sea p un número primo de la forma $4n+3$, demuéstrese que no existe $[x] \in U_p$ tal que $[x]^2 = [-1]$

Demostración

Supongamos que existe $[a] \in U_p$ tal que $[a]^2 = [-1]$ entonces $[a]^2 = [-1] \Rightarrow [a]^2[a]^2 = [a]^4 = [-1][-1] = [1] \Rightarrow o([a])|4 \Rightarrow$ existen tres casos

1. $o([a]) = 1$ entonces $[a] = 1$ lo cual es una contradicción.
2. $o([a]) = 2$ entonces $[a]^2 = 1$ lo cual también es una contradicción y por último;
3. $o([a]) = 4$ que es el único caso favorable.

Por lo tanto $o([a]) = 4$
Entonces $4 = ([a])|o(U_p) = p - 1 \Rightarrow 4|p-1 \Rightarrow 4|4n+3$ lo cual es una contradicción pues 4 no divide a $4n+3$
Por lo tanto no existe $[a] \in U_p$ tal que $[a]^2 = [-1]$.

q.e.d.

3. ¿Es alguno de los grupos $U_{18}, U_{20}, cíclico$?

Respuesta

$U_{18} = \{[1], [5], [7], [11], [13], [17]\}$
$U_{20}\{[1], [3], [7], [11], [13], [17], [19]\}$
Por lo que $o(U_{18}) = 6$ y $o(U_{20}) = 7$
Por lo tanto U_{20} es cíclico. Por el siguiente inciso (4).

4. Si p es primo. Demuestre que U_p es cíclico.

Demostración

Como U_p es un grupo abeliano finito, entonces $\forall[a] \in U_p \ [a]^{\varphi(p)} = [a]^{p-1} = [1]$, es decir, [a] satisface la ecuación $x^{p-1} = 1$.

Afirmamos que $x^{p-1} = 1$ tiene a lo más $p-1$ soluciones. Pues si $x^{p-1} = 1$ tuviera p soluciones entonces al fijarnos en el grupo $\mathbb{Z}/p\mathbb{Z}$, es decir:

$$\forall[b] \in \mathbb{Z}/p\mathbb{Z} \quad [b]^p = [0] \Rightarrow [b]^{p-1}[b] = 0 \quad \Rightarrow$$

$\mathbb{Z}/p\mathbb{Z}$ tendría divisores de cero.
Así $x^{p-1} = 1$ tiene $p-1$ soluciones.
Luego, por el ejercicio 9 de la lista 1.7, U_p es cíclico.

q.e.d.

6. Demuestre que si $a > 1$ es un entero entonces para cualquier natural n, $n|\varphi(a^n - 1)$.

Demostración

Se tiene que $[a] \in U_{a^n-1}$ pues $1 = (a^n - 1)(-1) + a(a^{n-1})$.
Además se tiene que $o([a]) = n$, pues $a^n \equiv 1 \mod (a^n - 1)$ y n es el mínimo, pues si $k < n$ tal que $a^k \equiv 1 \mod (a^n - 1)$ se tendría que $a^n - 1 | a^k - 1$ lo cual es imposible.
Por lo tanto con $o([a]) = n \Rightarrow n|\varphi(a^n - 1)$

q.e.d.

7. Demuestre que si $2^n - 1$ es primo, entonces

1. $(n, 2^n - 1) = 1$
2. $2^n - 1$ divide a $n^{2^n-2} - 1$

Demostración

1) Por 6) $n|\varphi(2^n - 1) \Rightarrow n|(2^n - 1) - 1 \Rightarrow n|2^n - 2$ ya que $2^n - 1$ es primo, y entonces $n \nmid 2^n - 1$.
Por lo tanto $(n, 2^n - 1) = 1$
(2)) Pendiente.

q.e.d.

10. Sea G un grupo tal que G/Z es cíclico, pruebe que G es abeliano.

Demostración

Como $G/Z(G)$ es cíclico entonces $G/Z(G) =< Z(G)g >$ para algún $g \in G$ fijo.
Sean $a, b \in G$, veamos que $ab = ba$. Consideremos a $Z(G)a$, $Z(G)b$, entonces:
$Z(G)a = (Z(G)g)^t$ para algún $t \in \mathbb{Z}$
$\Leftrightarrow Z(G)a = Z(G)g^t$ para algún $t \in \mathbb{Z}$
$\Leftrightarrow ag^{-t} \in Z(G)$ para algún $t \in \mathbb{Z}$
$\Rightarrow$ existe $z_1 \in Z(G)$ tal que $ag^{-t} = z_1$ para algún $t \in \mathbb{Z}$
$\Rightarrow a = z_1 g^t$
y $Z(G)b = (Z(G)g)^s$ para algún $s \in \mathbb{Z}$
$\Leftrightarrow Z(g)b = Z(G)g^s$ para algún $t \in \mathbb{Z}$
$\Leftrightarrow bg^{-s} \in Z(G)$ para algún $t \in \mathbb{Z}$
$\Rightarrow$ existe $z_2 \in Z(G)$ tal que $bg^{-s} = z_2$
$\Rightarrow b = z_2 g^s$.

Entonces:

$$\begin{aligned} ab &= z_1 g^t z_2 g^s \\ &= z_1 z_2 g^t g^s \\ &= z_1 z_2 g^{t+s} \\ &= z_1 z_2 g^{s+t} \\ &= z_2 z_1 g^s g^t \\ &= z_2 g^s z_1 g^t \\ &= ba \end{aligned} \tag{1}$$

Por lo tanto G es abeliano.

q.e.d.