UNIVERSIDAD SERGIO ARBOLEDA

Matemáticas

Teoría de Números

Corrección Parcial

Alexander Mendoza

12 de marzo de 2024

Parcial teoría de números

1. Demuestre que todo número de la forma $n^3 + 2n$ con $n \in \mathbb{N}$ es divisible por 3. Procederemos por inducción. Consideremos primero cuando $n = 1$

$$3 \mid 1^3 + 2 \cdot 1 = 3$$

   Con esto, se tiene que la propiedad se cumple para el caso base $n = 1$. Supongamos ahora que $3 \mid n^3+2n$ para algún n. Esta será nuestra hipótesis de inducción. Luego, por hipótesis de inducción, $3 \mid n^3$ y $3 \mid 2n$. Como $\gcd(3, 2) = 1$, entonces tenemos que $3 \mid n$, luego $3 \mid n^3$, $3 \mid 3n^2$, $3 \mid 5n$, $3 \mid 3$ por lo tanto $3 \mid n^3+3n^2+5n+3$ lo que implica que $3 \mid (n+1)^3+2(n+1)$.

2. Sean $a, b \in \mathbb{Z}^+$, demostrar que $lcm(a, b) \gcd(a, b) = ab$.

   Consideremos los siguientes casos:

   a) Cuando a, b son ambos primos: Como a, b son primos, tenemos que $\gcd(a, b) = 1$. Además sabemos que $lcm(a, b) = ab$. Con esto podemos concluir que $lcm(a, b)gcd(a, b) = ab \cdot 1 = ab$.

   b) Cuando a es primo y b no lo es: Sabemos que b no es primo, por lo tanto b es producto de primos, así $p_1^{m_1} p_2^{m_2} \cdot \cdots \cdot p_n^{m_n}$ si $a = P_k^{m_k}$ para algún k, concluimos que $\gcd(a, b) = a$ y $lcm(a, b) = b$, por lo tanto $lcm(a, b)gcd(a, b) = ab$. De manera análoga se puede demostrar cuando a no es primo y b es primo

   c) Cuando a, b son no primos: Entonces, tenemos:

$$\begin{aligned}\gcd(a, b) &= p_1^{\text{mín}(m_1,n_1)} \cdot p_2^{\text{mín}(m_2,n_2)} \cdot \dots \cdot p_k^{\text{mín}(m_k,n_k)}\\ \text{lcm}(a, b) &= p_1^{\text{máx}(m_1,n_1)} \cdot p_2^{\text{máx}(m_2,n_2)} \cdot \dots \cdot p_k^{\text{máx}(m_k,n_k)}\end{aligned}$$

   Por lo tanto,

$$\begin{aligned}&\gcd(a, b) \cdot \text{lcm}(a, b)\\ &= \left(p_1^{\text{mín}(m_1,n_1)} \cdot p_2^{\text{mín}(m_2,n_2)} \cdot \dots \cdot p_k^{\text{mín}(m_k,n_k)}\right) \cdot\\ &\left(p_1^{\text{máx}(m_1,n_1)} \cdot p_2^{\text{máx}(m_2,n_2)} \cdot \dots \cdot p_k^{\text{máx}(m_k,n_k)}\right)\\ &= (p_1^{m_1} \cdot p_1^{n_1}) \cdot (p_2^{m_2} \cdot p_2^{n_2}) \cdot \dots \cdot (p_k^{m_k} \cdot p_k^{n_k})\\ &= \left(p_1^{m_1+n_1}\right) \cdot \left(p_2^{m_2+n_2}\right) \cdot \dots \cdot \left(p_k^{m_k+n_k}\right)\\ &= a \cdot b\end{aligned}$$

3. Sea p primo. Demostrar que $\phi(p^r) = p^r - p^{r-1}$. Emplee este resultado para probar que si $2 \mid n$ entonces $\phi(2n) = 2\phi(n)$.

   Sea $N = \{n \mid 1 \leq n \leq p^a\}$, si logramos construir un conjunto P tal que P contenga todos los enteros positivos menores que p^a que no son primos relativos de p^a, entonces $|N| - |P| = \phi(p^r)$. Note que todo número de la forma xp no es primo relativo de p^a, ya que $\gcd(xp, p^a)$ es como mínimo p. De esta manera tenemos que $1p, 2p, ..., p^{a-1}p$ no son primos relativos de p^a, así tenemos que $P = \left\{mp \mid 1 \leq m \leq p^{a-1}\right\}$ y con esto, $|P| = p^{a-1}$, además sabemos que $|N| = p^a$, por lo tanto $\phi(p^r) = p^a - p^{a-1}$.

Teorema 1 *Si* $\gcd(m,n) = 1$, *entonces* $\phi(mn) = \phi(m)\phi(n)$

Para demostrar que si $2 \mid n$ entonces $\phi(2n) = 2\phi(n)$, procederemos de la siguiente manera. Sabemos que como $2 \mid n$, $n = 2^r m$ donde $\gcd(2,m) = 1$, así

$$
\begin{aligned}
\phi(2n) &= \phi(2^r m) && \\
&= \phi(2^{r+1})\phi(m) && \text{Por T.1 y } \gcd(2^r, m) = 1 \\
&= (2^{r+1} - 2^r)\phi(m) && \text{Por demostración anterior} \\
&= (2(2^r - 2^{r-1}))\phi(m) && \text{Propiedad distributiva} \\
&= 2\phi(2^r)\phi(m) && \text{Por demostración anterior} \\
&= 2\phi(2^r m) && \text{Por T.1} \\
&= 2\phi(n) &&
\end{aligned}
$$

4. Hallar el menor número positivo n con 42 divisores.

   Sabemos que la descomposición en primos de 42 es $\{2, 3, 7\}$, con esto, por el teorema de la función de divisores, tenemos que $n = p_1^1 p_2^2 p_3^6$ tiene 42 divisores, para p_1, p_2, p_3. Si tomamos los menores primos y los ordenamos de manera que $n = 5^1 * 3^2 * 2^6 = 2880$, con esto 2880 tiene 42 divisores y es el menor número con dicha propiedad.

5. Si p y q son primos tales que $p, q \geq 5$ demostrar que $24 \mid p^2 - q^2$.
   Dado que p y q son primos mayores o iguales que 5, ambos son impares. Podemos representarlos como $p = 2n + 1$ y $q = 2m + 1$, donde n y m son enteros no negativos.

   La diferencia de cuadrados $p^2 - q^2$ es:

$$
\begin{aligned}
p^2 - q^2 &= (2n+1)^2 - (2m+1)^2 \\
&= 4(n^2 - m^2) \\
&= 4(n-m)(n+m)
\end{aligned}
$$

   Como p y q son primos distintos, al menos uno de ellos es congruente a ± 1 módulo 3. Sin pérdida de generalidad, supongamos que p es congruente a 1 o -1 módulo 3. Entonces, p^2 es congruente a 1 módulo 3, al igual que q^2.

   Por lo tanto, $p^2 - q^2$ es la diferencia de dos números congruentes a 1 módulo 3, lo que implica que $p^2 - q^2$ es divisible por 3.

Además, como p y q son impares, p^2 y q^2 son congruentes a 1 módulo 8, lo que significa que $p^2 - q^2$ es divisible por 8.

Por lo tanto, $p^2 - q^2$ es divisible por tanto 3 como 8, y por ende, por 24. Por lo tanto, si p y q son primos mayores o iguales que 5, entonces 24 divide a $p^2 - q^2$.