Algebra Superior, 16.11.99

Examen Parcial num. 2

Sean a, b y n enteros con $n > 1$.

1. Define:
   (a) a es primo relativo a n.
   (b) $b \equiv a \pmod{n}$.
   (c) a es invertible mod n.

2. Demuestra:
   (a) a es invertible mod n si y solo si es primo relativo a n.
   (b) Si $b \equiv a \pmod{n}$, entonces a es invertible mod n si y solo si b es invertible mod n.

3. (a) Encuentra todos los enteros invertibles mod 9.
   (b) Sea $\phi(n)$ la función de Euler (el número de residuos invertibles mod n.) Encuentra $\phi(100)$.

4. (a) Supón que a es primo relativo a n. Define: el orden de $a \pmod{n}$.
   (b) Demuestra: el orden de $a \pmod{n}$ divide a $\phi(n)$. (Nota: se peude usar el teorema de Euler: $a^{\phi(n)} \equiv 1 \pmod{n}$.)
   (c) Encuentra el orden de $3 \pmod{100}$.

5. (Opcional, solo si te queda tiempo). Sea n libre de cuadrados (no lo divide ningun entero de la forma k^2). Demuestra que $N_1 \equiv N_2 \pmod{\phi(n)}$ implica $a^{N_1} \equiv a^{N_2} \pmod{n}$.