Universidad de la República - Facultad de Ingeniería - IMERL. Matemática Discreta 2

Examen - 13 de febrero de 2015. Duración: 4 horas.

N° de examen	Cédula	Apellido y nombre

Ejercicio 1.

a. Probar que si $1 \leq n \leq 130$ y $n = a \cdot b$, con a, b naturales, entonces $a \leq 11$ o $b \leq 11$.

b. Listar todos los primos menores o iguales a 130, explicando brevemente el método utilizado.

c. Un coleccionista de discos tiene 3860 dolares que piensa gastar en discos. Los precios de los discos que le interesan de su tienda favorita son de 238 dolares y 178 dolares. ¿Cúantos discos puede comprar el coleccionista utilizando todo el dinero?

Ejercicio 2.

a. Hallar $x \equiv 79^{221} \pmod{81}$, con $0 \leq x < 81$.

b. Hallar el mínimo x positivo tal que $x \equiv 11^{181} \pmod{595}$.

Ejercicio 3.

a. Sea $n = 86$.

i) Hallar el orden de 9 módulo n, es decir el orden de $\overline{9} \in U(n)$.

ii) Hallar una raíz primitiva módulo n.

b. Amanda y Benito quieren pactar una clave común utilizando el protocolo Diffie-Hellman. Eligen el primo $p = 997$ y la raíz primitiva $g = 7$. Amanda elige el número $m = 504$ y le envía a Benito el número 994. Benito elige el número $n = 12$. ¿Cúal es la clave común que eligieron Amanda y Benito?

Ejercicio 4.

a. Enunciar y demostrar el teorema de Lagrange para grupos.

b. Sea G un grupo finito.

i) Probar que $o(g) \mid |G|$ para todo $g \in G$.

ii) Probar que si $k \equiv l \pmod{|G|}$ entonces $g^k = g^l$ para todo $g \in G$.

iii) Sea $g \in G$ tal que $g^k = g^l$. Probar o refutar que $k \equiv l \pmod{|G|}$.