Algebra Superior, 23.9.99.

Tarea No. 7 (Para entregar el 30 de Septiembre de 1999.)

1. Sean a y b dos enteros positivos con $a \geq b$. Dividimos a entre b con residuo r, $0 \leq r < b$. Demuestra que $(a,b) = (b,r)$.

2. Aplica el algoritmo de Euclides para encontrar el máximo común divisor de 1998 y 2998.

3. Demuestra que en la sucesión de Fibonacci, 1, 2, 3, 5, 8, 13,..., en donde cada término, empezando con el tercero, es la suma de los dos anteriores, cada dos elementos consecutivos son primos relativos.

4. Otra demostración que hay una infinidad de números primos:
a) Demuestra que para a par y $m \neq n$, $a^{2^m}+1$ y $a^{2^n}+1$ son primos relativos (Sugerencia, si $m < n$, demuestra que $a^{2^m}+1$ divide a $a^{2^n}-1$. Usa el algoritmo de Euclides).
b) Deduce de a) que hay una infinidad de primos. (Sugerencia: Para a par considera la sucesión infinita: a^2+1, $a^{2^2}+1$, $a^{2^3}+1$, $\ldots$).

5. Demuestra que la sucesión 3, 7, 11, 15, 19, ... (i.e. todos los números de la forma $4k+3$) contiene a una infinidad de primos.

(Sugerencia: se puede usar la idea de la demostración de Euclides para la existencia de infinidad de primos; suponte que $p_1, p_2, p_3, ..., p_n$ son primos de dicha forma. Considera el número $N = 4 \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_n + 3$. Demuestra que todos los primos que aparecen en la factorización prima de N son "nuevos", i.e. fuera de la lista $p_1, p_2, p_3, ..., p_n$, y que al menos uno de ellos tiene que ser de la forma $4k+3$.)

6. Considera el conjunto de "números"

$$A = \{n + m\sqrt{-6} \mid n, m \in \mathbf{Z}\}.$$

El producto de números en A se define usando la regla $\sqrt{-6} \cdot \sqrt{-6} = -6$. Decimos que un número $z \in A$ es compuesto si existen $z_1, z_2 \in A$, distintos de 1, 0 o -1, tal que $z = z_1 \cdot z_2$. Un número que no es compuesto y no es 1, 0 o -1 se llama primo.
a) Demuestra que cada número $z \in A$, distinto de 1, 0 o -1, se puede factorizar como un producto de primos.
b) Demuestra que la factorización en primos no es única en A. Mas preciso: existen elementos $z \in A$ tal que se puede escribir a z como un producto de primos de A de dos maneras, y tal que hay factores de uno de los productos que no son iguales a ninguno de los factores del otro producto, ni a sus negativos.

(Sugerencia: define la *norma* de un número en A por $N(a + b\sqrt{-6}) = a^2 + 6b^2$. Demuestra que la norma satisface la identidad $N(z_1 \cdot z_2) = N(z_1)N(z_2)$. Demuestra el inciso a) por inducción sobre la norma de z. Para el inciso b) se puede encontrar un contra-ejemplo no muy grande...).