Álgebra II
Segundo Cuatrimestre — 2006

Factorización de enteros de Gauss

1. Sea $p \in \mathbb{Z}$ un primo. Si $a + bi$ divide a p en $\mathbb{Z}[i]$, entonces $a - bi$ también.
2. Sea $p \in \mathbb{Z}$ un primo. Entonces o bien p es primo en $\mathbb{Z}[i]$ o bien $p = (a + bi)(a - bi)$ con $a + bi$ (y por lo tanto $a - bi$) primo en $\mathbb{Z}[i]$.
3. Sea $a + bi$ primo en $\mathbb{Z}[i]$. Entonces $(a + bi)(a - bi)$ es o bien un entero primo o bien el cuadrado de un entero primo.
4. Sea $p \in \mathbb{Z}$ un primo. Son equivalentes
   a) p es primo en $\mathbb{Z}[i]$.
   b) El anillo $\mathbb{Z}[i]/(p)$ es un cuerpo.
   c) El polinomio $x^2 + 1$ es irreducible en $\mathbb{Z}_p[x]$.
5. Sea $p \in \mathbb{Z}$ un primo impar y sea $a \in \mathbb{Z}_p$.
   a) $a^2 = -1$ en $\mathbb{Z}_p$ si y sólo si el orden de a en $\mathbb{Z}_p^*$ es 4.
   b) $\mathbb{Z}_p^*$ tiene elementos de orden 4 si y sólo si p es congruente con 1 módulo 4.
6. Sea $p \in \mathbb{Z}$ un primo. Son equivalentes
   a) $p = (a + bi)(a - bi)$ con $a + bi$ primo en $\mathbb{Z}[i]$.
   b) $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$.
   c) -1 es un cuadrado en $\mathbb{Z}_p$.
   d) $p = 2$ o p es congruente con 1 módulo 4.
7. Los enteros primos que son primos en $\mathbb{Z}[i]$ son aquellos congruentes con 3 módulo 4.
8. **Receta para factorizar un entero de Gauss.**
   a) Si $x \in \mathbb{Z}$, factorizar a x como producto de primos en $\mathbb{Z}$. Luego factorizar los primos congruentes con 1 módulo 4.
   b) Si $x = a + bi$, con $b \neq 0$ y a y b coprimos, entonces en la factorización de x no aparecen enteros primos.
   c) Con las mismas hipótesis del item anterior considerar el entero $y = x\overline{x}$. Entonces cada entero primo en la factorización de y es congruente a 1 módulo 4 y por lo tanto se escribe como $z\overline{z}$, con z primo en $\mathbb{Z}[i]$. Entonces z/x o $\overline{z}/x$ en $\mathbb{Z}[i]$.
   d) Si $x = a + bi$ con $b \neq 0$ y a y b no coprimos escribir $x = dx'$, donde $d = (a, b)$. Entonces x se factoriza factorizando d y x'.
   e) Pídale a un compañero que escriba un entero de Gauss y factorícelo.