is a unit in R then $U = R$ (see Problem 5). If, on the other hand, x is a unit in R, then $x^{-1} \in R$ and the relation $a_0 = xu_0$ becomes $u_0 = x^{-1}a_0 \in A$ since A is an ideal of R. This implies that $U \subset A$; together with $A \subset U$ we conclude that $U = A$. Therefore there is no ideal of R which fits strictly between A and R. This means that A is a maximal ideal of R.

Problems

1. In a commutative ring with unit element prove that the relation a is an associate of b is an equivalence relation.
2. In a Euclidean ring prove that any two greatest common divisors of a and b are associates.
3. Prove that a necessary and sufficient condition that the element a in the Euclidean ring be a unit is that $d(a) = d(1)$.
4. Prove that in a Euclidean ring (a, b) can be found as follows:

$$\begin{aligned} b &= q_0 a + r_1, \quad \text{where} \quad d(r_1) < d(a) \\ a &= q_1 r_1 + r_2, \quad \text{where} \quad d(r_2) < d(r_1) \\ r_1 &= q_2 r_2 + r_3, \quad \text{where} \quad d(r_3) < d(r_2) \\ &\vdots \qquad\qquad\qquad\qquad \vdots \\ r_{n-1} &= q_n r_n \end{aligned}$$

and $r_n = (a, b)$.

5. Prove that if an ideal U of a ring R contains a unit of R, then $U = R$.
6. Prove that the units in a commutative ring with a unit element form an abelian group.
7. Given two elements a, b in the Euclidean ring R their *least common multiple* $c \in R$ is an element in R such that $a \mid c$ and $b \mid c$ and such that whenever $a \mid x$ and $b \mid x$ for $x \in R$ then $c \mid x$. Prove that any two elements in the Euclidean ring R have a least common multiple in R.
8. In Problem 7, if the least common multiple of a and b is denoted by $[a, b]$, prove that $[a, b] = ab/(a, b)$.

3.8 A Particular Euclidean Ring

An abstraction in mathematics gains in substance and importance when, particularized to a specific example, it sheds new light on this example. We are about to particularize the notion of a Euclidean ring to a concrete ring, the ring of Gaussian integers. Applying the general results obtained about Euclidean rings to the Gaussian integers we shall obtain a highly nontrivial theorem about prime numbers due to Fermat.

Prof. Carlos Alberto López Andrade
Materia: Anillos y Campos

I) Find all the units in $\mathbb{Z}[i]$.

II) If $a + bi$ is not a unit of $\mathbb{Z}[i]$ prove that $a^2 + b^2 > 1$.

III) Let $\pi \in \mathbb{Z}[i]$ be such that $d(\pi) = p$, where p is a prime in $\mathbb{Z}$. Show that π is a prime of $\mathbb{Z}[i]$.

IV) Show that 2 is equal to the product of a unit and the square of a prime in $\mathbb{Z}[i]$.

V) Consider $\alpha = 7 + 2i$ and $\beta = 3 - 4i$ in $\mathbb{Z}[i]$. Find σ and ρ in $\mathbb{Z}[i]$ such that $\alpha = \beta\sigma + \rho$ with $d(\rho) < d(\beta)$.

VI) Use a Euclidean algorithm in $\mathbb{Z}[i]$ to find a $\gcd$ of

a) $8 + 6i$ and $5 - 15i$ in $\mathbb{Z}[i]$.

b) $3 + 4i$ and $4 - 3i$ in $\mathbb{Z}[i]$.

Puebla, Pue., a 5 de marzo de 2018