Lisbon Summer School (2011) Problem Set 1

Keith Conrad

1. Let p be a prime number (that is, a positive prime in $\mathbf{Z}$).

   a) Factor 2, 5, 13, 17, and 29 into primes in $\mathbf{Z}[i]$.

   b) Show that if p is a sum of two squares in $\mathbf{Z}$ then p is not prime in $\mathbf{Z}[i]$.

   c) Show that if p is not prime in $\mathbf{Z}[i]$ then p is a sum of two squares in $\mathbf{Z}$. Thus the converse to part b is true. (Hint: Write $p = \alpha\beta$ where α and β are not ± 1 or $\pm i$ and take the norm of both sides to get an equation in $\mathbf{Z}^+$.)

   Thus the prime numbers which stay prime in $\mathbf{Z}[i]$ are the ones which are not a sum of two squares (like 3, 7, 11,. . .).

2. The integer 65 is a sum of two squares in two different ways: $65 = 1^2 + 8^2 = 4^2 + 7^2$. We will see how this is related to factorization in $\mathbf{Z}[i]$.

   a) Give a prime factorization of $65 = 5 \cdot 13$ in $\mathbf{Z}[i]$ based on factoring 5 and 13 first.

   b) In $\mathbf{Z}[i]$, $1^2 + 8^2 = (1 + 8i)(1 - 8i)$. Find prime factorizations of $1 + 8i$ and $1 - 8i$ in $\mathbf{Z}[i]$. (Hint: Since $1 + 8i$ has norm 65, try to write it as a product of a number of norm 5 and a number of norm 13.)

   c) In $\mathbf{Z}[i]$, $4^2 + 7^2 = (4 + 7i)(4 - 7i)$. Find prime factorizations of $4 + 7i$ and $4 - 7i$ in $\mathbf{Z}[i]$.

   d) Explain how the Gaussian prime factorizations of $5 \cdot 13$, $(1+8i)(1-8i)$, and $(4+7i)(4-7i)$ can be matched term-by-term using multiplication by ± 1 or $\pm i$.

   e) Use factorizations in $\mathbf{Z}[i]$ to discover an integer which is a sum of two squares in three different ways and then find one which is a sum of two squares in four different ways.

3. Assuming $\mathbf{Z}[i]$ has unique factorization, show that if α and β are relatively prime Gaussian integers such that $\alpha\beta = \gamma^n$ for some $n \geq 2$ and $\gamma \in \mathbf{Z}[i]$ then $\alpha = u\lambda^n$ and $\beta = v\mu^n$ where λ and μ are in $\mathbf{Z}[i]$ and u and v are ± 1 or $\pm i$. In words, if two relatively prime Gaussian integers have a product that is an nth power then the two factors are each nth powers up to multiplication by ± 1 or $\pm i$.

4. a) Use unique factorization in $\mathbf{Z}[i]$ to show by contradiction that the equation $y^2 = x^3 - 9$ has no integral solutions. (Hint: The only elements of norm 9 are ± 3 and $\pm 3i$.)

   b) Use unique factorization in $\mathbf{Z}[i]$ to show the only integral solutions of the equation $y^2 = x^3 - 121$ are $(5, \pm 2)$. (Note: this equation has infinitely many *rational* solutions, two examples being $(89/4, 835/8)$ and $(4217/529, 238912/12167)$.)

   b) Use unique factorization in $\mathbf{Z}[i]$ to find all the integral solutions of the equation $y^2 = x^3 - 49$.