Gaussian Integers – Square Dance (*Circle in a Box* Chapter 13)

1. Let $\alpha = 10 - 11i$ and $\beta = 3 - 2i$. Compute $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and α/β.

2. If $\alpha = a + bi$, its conjugate is $\overline{\alpha} = a - bi$. Confirm that both $\alpha + \overline{\alpha}$ and $\alpha\overline{\alpha}$ are ordinary integers.

3. Demonstrate that $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ and that $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$.

4. We define the *norm* of $\alpha = a + bi$ as $N(\alpha) = \alpha^2 + \beta^2$. (The norm measures how "large" α is in some sense). Determine $N(2 + 5i)$ and $N(1 - i)$. Now multiply $(2 + 5i)(1 - i)$ and compute the norm of the result. What do you notice?

5. Use properties of conjugates to prove that in general we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

6. Find all Gaussian integers α for which $N(\alpha) = 1$. (There are four of them, called the units. Every Gaussian integer is divisible by these four numbers – check this!)

7. Now find all α such that $N(\alpha) = 5$. Then try $N(\alpha) = 7$ and $N(\alpha) = 25$. (There are twelve answers for the latter question. Don't forget that $N(-5) = 25$, for example).

8. Find a way to write $1 + 3i$ as a product of two non-trivial factors. In other words, don't use the units from Exercise 6 which divide all Gaussian integers.

9. We know that 29 can be written as the sum of two squares. How does this lead to a way to write 29 as a product of two Gaussian integers?

10. Next find a way to write $2 + 9i$ as a product of two non-trivial factors. HINT: use the norm.

11. Show that $4 + i$ and 11 are prime Gaussian integers by considering the norm of each.

12. Now suppose that $p \equiv 1 \mod 4$ (i.e. p is one greater than a multiple of four.) We know that $1 \cdot 2 \cdot 3 \cdots (p - 2)(p - 1) \equiv (-1) \mod p$ by Wilson's theorem. Use this result to explain why $\left[1 \cdot 2 \cdot 3 \cdots \frac{(p-1)}{2}\right]^2 + 1$ is a multiple of p.

13. It is a fact that if a Gaussian prime divides $\alpha\beta$, then it must divide either α or β. The previous question implies that there is some number n such that $n^2 + 1$ is divisible by p. In other words, p divides $(n + i)(n - i)$. Explain why neither factor is divisible by p. Conclude that p is not a Gaussian prime.

14. We just saw that if $p \equiv 1 \mod 4$, then p is not prime in the Gaussian integers. Thus we can write $p = \alpha\beta$ for nontrivial numbers α and β. Explain why this means that $N(\alpha) = p$, and then deduce that $p = a^2 + b^2$ for some ordinary integers a and b. Thus p is suave!