M3P14 EXAMPLE SHEET 3

1. Give the prime factorizations, in $\mathbb{Z}[i]$, of the following elements of $\mathbb{Z}[i]$. Be sure to justify that each of the factors is prime!

1a. 51

1b. $8 + i$

1c. $5 + 7i$

2. Find a greatest common divisor, in $\mathbb{Z}[i]$, of the following elements of $\mathbb{Z}[i]$:

2a. 51 and $20 + 5i$

2b. 95 and $8 + i$

3a. Let n be an integer. Show that if $4n$ is the sum of three squares, then so is n. [HINT: if $4n = a^2 + b^2 + c^2$, show that all of a, b, and c must be even.]

3b. Show that if n has the form $4^t(8k + 7)$ for some nonnegative integer t and integer k, then n cannot be written as the sum of three squares. (In fact, these are the *only* numbers that cannot be written as the sum of three squares, but this is much harder.)

4. Prove Wilson's theorem: If p is prime, then $(p-1)! \equiv -1 \pmod{p}$. [Hint: when multiplying together all the nonzero congruence classes mod p, almost every class cancels with its inverse. Which ones don't?]

5. Use Fermat descent, starting with $557^2 + 55^2 = 26 \cdot 12049$ to write the prime 12049 as the sum of two squares.

6. For each of the following n, either write n as the sum of two squares, or prove that it is not possible to do so: 1865, 77077, 609, and 7501.

7. Let $\zeta = \frac{-1}{2} + \frac{\sqrt{-3}}{2}$, and let $\mathbb{Z}[\zeta]$ be the subset of $\mathbb{C}$ consisting of all complex numbers of the form $a + b\zeta$, where a, b are integers.

7a. Show that $\mathbb{Z}[\zeta]$ is closed under addition and multiplication.

7b. Let $N : \mathbb{Z}[\zeta] \to \mathbb{C}$ be defined by $N(z) = z\overline{z}$. Show that if $z \in \mathbb{Z}[\zeta]$, then $N(z)$ is an integer.

7c. Show that for any $a, b \in \mathbb{Z}[\zeta]$, with $b \neq 0$, there exist a q,r in $\mathbb{Z}[\zeta]$ such that $a = bq + r$ and $N(r) < N(b)$.

7d. Conclude that for any a, b in $\mathbb{Z}[\zeta]$, a greatest common divisor of a and b exists.