# UNIQUE FACTORIZATION AND FERMAT'S LAST THEOREM
# HOMEWORK 3

**Problem 1.** Prove that $\mathbf{Z}[\sqrt{-2}]$ is a principal ideal domain. [Hint: prove that division with remainder works in $\mathbf{Z}[\sqrt{-2}]$ for the same reason that it works in $\mathbf{Z}[\zeta]$]

**Problem 2 (Imaginary quadratic integer rings are integrally closed).** Let $D \geq 2$ be a squarefree integer. A complex number of the form $z = a + b\sqrt{-D}$ with $a, b \in \mathbf{Q}$ is called an *algebraic integer* if it is a root of a monic polynomial $f(X) = X^2 + tX + n$ with $t, n \in \mathbf{Z}$.

(i) Prove that $z^2 - (z + \overline{z})\, z + |z|^2 = 0$ for any $z \in \mathbf{C}$.
(ii) Prove that any element $z \in R$ is an algebraic integer.
(iii) Let $z = a + b\sqrt{-D}$ with $a, b \in \mathbf{Q}$. Prove that if $z$ is an algebraic integer then $z \in R$.

Hence $R$ is exactly the set of algebraic integers in the field $\mathbf{Q}(\sqrt{-D}) = \{a + b\sqrt{-D} \ : \ a, b \in \mathbf{Q}\}$.

**Problem 3 (Irreducible and prime elements).** Let $R$ be an imaginary quadratic integer ring.

(i) Prove that a prime element in $R$ is irreducible.
(ii) Prove that any nonzero non-unit in $R$ is a product of irreducible elements of $R$. In other words, irreducible factorizations always exist in $R$.
(iii) Prove that if all irreducible elements of $R$ are prime, then prime factorizations in $R$ are unique up to reordering and multiplication by units.

**Problem 4 (Non-unique factorizations in $\mathbf{Z}[\sqrt{-5}]$).** Let $R = \mathbf{Z}[\delta]$ with $\delta = \sqrt{-5}$.

(i) Show that $2, 3, 1 + \delta$, and $1 - \delta$ are irreducible in $R$. [Hint: to show that $2$ is irreducible, for example, prove that there is no element $z \in R$ with $|z|^2 = 2$.]
(ii) Show that $2, 3, 1+\delta$, and $1-\delta$ are not prime in $R$. [Hint: use the fact that $6 = 2 \cdot 3 = (1+\delta)(1-\delta)$.]

**Problem 5 (Practice with ideal factorization).**

(i) Factor the ideal $(6)$ into prime ideals in $\mathbf{Z}[\sqrt{-6}]$.
(ii) Determine whether $11$ is irreducible and/or prime in $\mathbf{Z}[\sqrt{-5}]$.
(iii) Factor the principal ideal $(14)$ into prime ideals in $\mathbf{Z}[\sqrt{-5}]$. Be sure to prove that the factors of your ideal are prime!

**Problem 6 (The Main Lemma of ideal factorization).** Let $R$ be an imaginary quadratic integer ring. Recall that if $I \subset R$ is an ideal, its *complex conjugate* is $\overline{I} = \{\overline{z} \ : \ z \in I\}$.

(i) Prove that $\overline{I}$ is an ideal in $R$.

Recall from class that $I$ can be generated by two elements, say $I = (z, w)$. Then $\overline{I} = (\overline{z}, \overline{w})$ and $I\overline{I} = (z\overline{z}, z\overline{w}, \overline{z}w, w\overline{w})$.

(ii) Show that $z\overline{z}$, $w\overline{w}$, and $z\overline{w} + \overline{z}w$ are ordinary integers. Let $n \in \mathbf{Z}$ be their greatest common divisor.
(iii) Prove that $(n) \subset I\overline{I}$.
(iv) Prove that $n \mid z\overline{z}$ and $n \mid w\overline{w}$.
(v) Prove that $z\overline{w}/n$ and $\overline{z}w/n$ are algebraic integers in the sense of Problem 2. Conclude using Problem 2(iii) that $n$ divides $z\overline{w}$ and $\overline{z}w$ in $R$.
(vi) Prove that $I\overline{I} = (n)$.
(vii) *Extra credit*: Let $I$ be the ideal $(2, 1 + \sqrt{-3})$ of the ring $\mathbf{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \ : \ a, b \in \mathbf{Z}\}$. (Note that this is *not* the quadratic integer ring $\mathbf{Z}[\zeta]$!) Prove that $I\overline{I}$ is not a principal ideal.