Math 566 - Homework 5
Due Wednesday February 28, 2024

The assignment continues in the back.

1. The *Hilbert numbers* are the positive integers of the form $4n+1$, with $n \geq 0$,
$$\mathscr{H} = 1 + 4\mathbb{N}.$$
A *Hilbert prime* is a Hilbert number greater than 1 that is not divisible by any smaller Hilbert number except 1.
   (i) Let $a, b \in \mathscr{H}$. Show that $a \mid b$ in $\mathbb{Z}$ if and only if there exists $c \in \mathscr{H}$ such that $b = ac$. Thus, divisibility in $\mathscr{H}$ coincides with divisibily in $\mathbb{Z}$.
   (ii) Prove that a Hilbert number is a Hilbert prime if and only if it is either an integer prime of the form $4n+1$ (such as 5, 13, 17, etc), or an integer of the form $(4a+3)(4b+3)$ where both $4a+3$ and $4b+3$ are integer primes (for example, $21 = (3)(7)$).
   (iii) Let a be a Hilbert number greater than 1. Prove that a can be written as a product of Hilbert primes using strong induction: if a is a Hilbert prime, then we can write $a = a$. Otherwise, show there is a smallest Hilbert prime b such that $b \mid a$, and writing $a = bc$, apply the induction hypothesis to c.
   (iv) Using the above algorithm, factor 441 into Hilbert primes.
   (v) Find a different factorization of 441 into Hilbert primes. Conclude that the Hilbert numbers do not satisfy unique factorization.

2. Let R be a Euclidean domain with Euclidean function φ.
   (i) Prove that for all $r \neq 0$, $\varphi(1_R) \leq \varphi(r)$.
   (ii) Prove that $u \in R$ is a unit if and only if $\varphi(u) = \varphi(1_R)$.

Definition. Let R be a commutative ring with unity. A function $N\colon R \to \mathbb{N}$ is a *Dedekind-Hasse norm* if $N(a) \geq 0$ for all a, with equality if and only if $a = 0$; and for every nonzero $a, b \in R$, either $a \in (b)$ or there exists a nonzero element $c \in (a, b)$ with norm strictly smaller than that of b (that is, either b divides a, or there exist $s, t \in R$ such that $0 < N(sa - tb) < N(b)$.

3. Let R be an integral domain. Prove that if there is a Dedekind-Hasse norm N on R, then R is a PID. Hint: Given an nonzero ideal I, let b be a nonzero element of I with $N(b)$ minimal.

Definition. Let R be an integral domain. A nonzero nonunit $u \in R$ is said to be a *universal side divisor* if for every $x \in R$ there is a $z \in R$ such that z is either 0 or a unit, and u divides $x - z$; that is, there is a weak version of the division algorithm for u: every x can be written as $x = qu + z$, where z is either 0 or a unit.

4. Show that if R is a Euclidean domain that is not a field, then there are universal side divisors in R.

5. Let $\alpha = \frac{1+\sqrt{-19}}{2}$, and let $R = \mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$, which is a subring of $\mathbb{C}$. Define $N\colon R \to \mathbb{Z}$ by

$$N(a + b\alpha) = (a + b\alpha)(a + b\overline{\alpha}) = a^2 + ab + 5b^2,$$

where $\overline{\alpha}$ is the complex conjugate of α.

(i) Show that N is multiplicative: if $x, y \in R$, then $N(xy) = N(x)N(y)$.

(ii) Show that $N(x) \geq 0$ for all $x \in R$, and $N(x) = 0$ if and only if $x = 0$.

(iii) Show that x is a unit in R if and only if $N(x) = 1$.

(iv) Show that the only units of R are 1 and -1.

(v) Show that if $a, b \in \mathbb{Z}$, and $b \neq 0$, then $N(a + b\alpha) \geq 5$. Conclude that the smallest nonzero values of N are 1 and 4, and determine all $x \in R$ with $N(x) = 4$.

(vi) Show that both 2 and 3 are irreducible in R.

(vii) Show that if $u \in R$ is a universal side divisor, then $u = \pm 2$ or $u = \pm 3$.

(viii) Show that none of α, $\alpha + 1$, and $\alpha - 1$ are divisible by ± 2 or by ± 3.

(ix) Conclude that R does not have universal side divisors, and hence is not a Euclidean domain.

NOTE. One can show that N is a Dedekind-Hasse norm on R, so that R is a PID that is not a Euclidean domain.