Math 566 - Homework 5

SOLUTIONS

Prof Arturo Magidin

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 $\mathbb{Z}$.

Proof. Suppose that $a, b \in \mathscr{H}$, and there exists an integer c such that $b = ac$. Since a and b are both positive, so is c. And since $a \equiv 1 \pmod 4$ and $b \equiv 1 \pmod 4$, looking at the equation modulo 4 we obtain $1 \equiv 1(c) \pmod 4$. Thus, $c \equiv 1 \pmod 4$, and hence $c \in \mathscr{H}$. The converse (if a divides b in $\mathscr{H}$ then a divides b in $\mathbb{Z}$) is clear. This shows divisibility in $\mathscr{H}$ coincides with divisibility 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, $21 = (3)(7)$).

Proof. If p is a prime integer of the form $4n+1$, then it is in $\mathscr{H}$ and is not divisible by any integer greater than 1 and smaller than p, hence is not divisible by any Hilbert integer greater than 1 and smaller than p; thus, p is a Hilbert prime.

If $p = (4a+3)(4b+3)$, then $p \equiv 1 \pmod 4$ (since $9 \equiv 1 \pmod 4$) and thus lies in $\mathscr{H}$. The only positive integer divisors of p are 1, p, $4a+3$, and $4b+3$, and thus the only Hilbert numbers that divide p are 1 and p. Thus, p is a Hilbert prime. This completes the proof of sufficiency.

To prove necessity, let $m \in \mathscr{H}$, $m > 1$ be an integer that is not a prime of the form $4a+1$, and not of the form $(4a+3)(4b+3)$ with $4a+3$ and $4b+3$ both positive integer primes. If m is not an integer prime and is divisible by a prime $p \equiv 1 \pmod 4$, then $1 < p < m$, and $p \in \mathscr{H}$ also divides m in $\mathscr{H}$ So m is not a Hilbert prime. If all prime factors of m are congruent to 3 modulo 4, but is not a product of exactly two of them, then it is a product of an even number of such primes, and at least 4. Let p_1 and p_2 be two such primes with $p_1p_2 \mid m$. (We are not assuming $p_1 \neq p_2$). Since $m \neq p_1p_2$, then $1 < p_1p_2 < m$, and $p_1p_2 \equiv 1 \pmod 4$, so $p_1p_2 \in \mathscr{H}$. Thus, m is not a Hilbert prime. □

(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.

Proof. Assume all Hilbert numbers m greater than 1 and smaller than $k \in \mathscr{H}$ can be written as a product of Hilbert primes, $m = p_1p_2\cdots p_r$ with $p_1 \leq p_2 \leq \cdots \leq p_r$, and where p_i is the smallest Hilbert prime that divides $p_ip_{i+1}\cdots p_r$.

We prove that k can be written as a product of Hilbert primes in the same way. If k is a Hilbert prime, we write $k = k$ and we are done. If k is not a Hilbert prime, then there exist Hilbert numbers m, $1 < m < k$, such that m divides k. Let p be the smallest such Hilbert integer. I claim that p is a Hilbert prime.

Indeed, if p is not a Hilbert prime, then there exist a Hilbert number q, $1 < q < p$, such that $q \mid p$. But since $p \mid k$, it follows that $q \mid k$, contradicting the minimality of p. Thus, p is a Hilbert prime.

Since p divides k, we can write $k = pq$ with q a Hilbert number, $1 < q < k$. Applying the induction hypothesis to q, we can write q as a product of Hilbert primes, $q = q_1 q_2 \cdots q_s$, with $q_1 \leq q_2 \leq \cdots \leq q_s$, and where q_i is the smallest Hilbert prime that divides $q_i q_{i+1} \cdots q_s$.
Then $k = pq_1 \cdots q_s$; p is the smallest Hilbert prime that divides $k = pq_1 \cdots q_s$, each q_i is the smallest Hilbert prime that divides $q_i q_{i+1} \cdots q_s$. This proves k has a factorization as described, and we are done. □

(iv) Using the above algorithm, factor 441 into Hilbert primes.

Answer. The positive integer divisors of 441 are 1, 3, 7, 9, 21, 49, 63, 147, and 441. The ones that are Hilbert numbers are 1, 9, 21, 49, and 441. From (ii), we know that the primes among them are $9 = (3)(3)$, $21 = (3)(7)$, and $49 = (7)(7)$. The smallest is 9, and we write $441 = (9)(49)$. These are both Hilbert primes, so we are done. □

(v) Find a different factorization of 441 into Hilbert primes. Conclude that the Hilbert numbers do not satisfy unique factorization.

Answer. We can also factor $441 = (21)(21)$, and 21 is a Hilbert prime, as noted above. Thus, even though there is an algorithm that produces a unique factorization for every Hilbert integer, $\mathscr{H}$ do not satisfy unique factorization. □

2. Let R be a Euclidean domain with Euclidean function φ.

(i) Prove that for all $r \neq 0$, $\varphi(1_R) \leq \varphi(r)$.

Proof. Let $r \in R$, $r \neq 0$. Then $1_R r \neq 0$, so by the properties of the Euclidean function,

$$\varphi(1_R) \leq \varphi(1_R r) = \varphi(r). \qquad \square$$

(ii) Prove that $u \in R$ is a unit if and only if $\varphi(u) = \varphi(1_R)$.

Proof. If u is a unit, then there exists $v \in R$ such that $uv = 1$. Then $\varphi(1_R) \leq \varphi(u) \leq \varphi(uv) = \varphi(1_R)$, so we have $\varphi(u) = \varphi(1_R)$.
Conversely, if $\varphi(u) = \varphi(1_R)$, then applying the second part of the definition of Euclidean function to divide 1_R by u, we know there exists $q, r \in R$ such that $1_R = qu + r$, and $r = 0$ or $\varphi(r) < \varphi(u) = \varphi(1_R)$. But by (i), we know that if $r \neq 0$, then $\varphi(r) \geq \varphi(1_R)$, so we conclude that $r = 0$. Therefore, $1 = qu$, so u is a unit. □

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.

Proof. Let $I \triangleleft R$. If $I = (0)$, we are done. If $I \neq (0)$, then let $b \in I$ be an element such that $N(b)$ is minimal among nonzero elements of I. The claim is that $I = (b)$. We certainly have $(b) \subseteq I$.

Let $a \in I$; if $a = 0$, then $a \in (b)$. If $a \neq 0$, then, since N is a Dedekind-Hasse norm, either $a \in (b)$, or there exists $s, t \in R$ such that $0 < N(sa - tb) < N(b)$. However, $(a, b) \subseteq I$, so $sa - tb \in I$ for any $s, t \in R$. Thus, by the minimality of $N(b)$, either $sa - tb = 0$ or $N(sa - tb) \geq N(b)$. Thus, we must have that $a \in (b)$. This proves that $I \subseteq (b)$, as required. □

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.

   Proof. Assume that R is a Euclidean domain that is not a field. Then the set of nonzero nonunits is not empty, so there is a nonzero nonunit $u \in R$ such that $\varphi(u)$ is minimal among the values of the Euclidean function φ on nonzero nonunits. We claim that u is a universal side divisor.

   Indeed, let $x \in R$. Since R is a Euclidean domain, there exist q and r in R such that $x = qu + r$ and either $r = 0$ or $\varphi(r) < \varphi(u)$. By the minimality of $\varphi(u)$, r must be either 0 or a unit, so there exists z such that u divides $x - z$ and z is either 0 or a unit (namely $z = r$). This shows that u is a universal side divisor, as claimed. □

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 $N(xy) = N(x)N(y)$.
   Proof. Note that $N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2$, where $\overline{\alpha}$ is the complex conjugate of α and $|\alpha|$ is the complex norm of α. Thus,

$$N(\alpha\beta) = |\alpha\beta|^2 = (|\alpha|\,|\beta|)^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta). \quad \square$$

   (ii) Show that $N(x) \geq 0$ for all $x \in R$, and $N(x) = 0$ if and only if $x = 0$.
   Proof. Since $|\alpha| = 0$ if and only if $\alpha = 0$, and $|\alpha| \geq 0$, these conditions also hold for N. □

   (iii) Show that x is a unit in R if and only if $N(x) = 1$.
   Proof. If α is a unit, then $1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$, and since $N(\alpha)$ is a positive integer, we must have $N(\alpha) = 1$. Conversely, if $N(\alpha) = 1$, then $1 = \alpha\overline{\alpha}$, so $\overline{\alpha} = \alpha^{-1}$. Now we just notice that $\overline{\alpha} \in R$, since

$$\overline{\alpha} = a + b\left(\frac{1 - \sqrt{-19}}{2}\right) = (a + b) - b\left(\frac{1 + \sqrt{-19}}{2}\right).$$

   It follows that α is a unit in R. □

   (iv) Show that the only units of R are 1 and -1.
   Proof. Clearly, both 1 and -1 are units.

   For the converse, assume that $\alpha = a + b\left(\frac{1+\sqrt{-19}}{2}\right)$ is a unit in R, $a, b \in \mathbb{Z}$. Note that if $a, b \in \mathbb{Z}$, then

$$N\left(a + b\left(\frac{1 + \sqrt{-19}}{2}\right)\right) = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4}b^2.$$

   This is a sum of two squares. Therefore, in order for $N(\alpha)$ to be 1, we must have $b = 0$ (otherwse $N(\alpha) \geq \frac{19}{4} > 4$), and hence $a^2 = 1$. Thus, $\alpha = 1$ or $\alpha = -1$, as claimed. □

   (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 $N(x) = 4$.
   Proof. From the formula above, if $b \neq 0$, then $N(\alpha) \geq \frac{19}{4}b^2 \geq \frac{19}{4} > 4$. Since $N(\alpha)$ must be an integer, it follows that $N(\alpha) \geq 5$.

   On the other hand, when $b = 0$, we get $N(a) = a^2$. This can take values 1 and 4, which are smaller than the values the norm can take when $b \neq 0$. So the smallest values that N takes are 1 (when $|a| = 1$ and $b = 0$; i.e., at 1 and -1), and 4. The latter occurs when $|a| = 2$ and $b = 0$, i.e., at 2 and -2. □

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

Proof. If $2 = xy$ in R, then $N(2) = N(x)N(y)$. Thus, $4 = N(x)N(y)$. Since there is no $r \in R$ with $N(r) = 2$, this means that one of $N(x)$ and $N(y)$ is 1, and the other is 4. If $N(x) = 1$, then x is a unit; if $N(y) = 1$, then y is a unit. Thus, if $2 = xy$, then either x is a unit or y is a unit. Hence 2 is irreducible in R.

Similarly, if $3 = xy$, then $9 = N(3) = N(x)N(y)$; since there are no $r \in R$ with $N(r) = 3$, one of $N(x)$ or $N(y)$ is equal to 1, and therefore one of x or y is a unit. Thus, 3 is irreducible in R □

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

Proof. Suppose that u is a universal side divisor. Taking $x = 2$, it follows that u must divide either 2, $2 - 1$, or $2 + 1$ (since the only possible values for z are 0, 1, and -1). Since u is not a unit, then u must divide either 2 or 3; and as the only nonunit elements of R that divide 2 or divide 3 are ± 2 and ± 3, it follows that u would have to be one of 2, -2, 3, or -3. □

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

Proof. Note that $a + b\alpha$ is divisible by 2 (or -2) in R if and only if a and b are both even. In particular, neither α, $1 + \alpha$, nor $-1 + \alpha$ are multiples of 2 or -2. Similarly, $a + b\alpha$ is divisible by 3 or by -3 in R if and only if a and b are both multiples of 3, so none of α, $1 + \alpha$, nor $-1 + \alpha$ are divisible by 3 or -3. □

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

Answer. Suppose u is a universal side divisor. If we take $x = \alpha$, then u must divide either α, $\alpha - 1$, or $\alpha + 1$, and we just saw that none of ± 2 nor ± 3 divide α, $\alpha - 1$, or $\alpha + 1$. As these are the only possible values for universal side divisors by part (vii), it follows that R does not have universal side divisors. Since Euclidean domains always have universal side divisors, we conclude that R 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.