QUESTION:(HD0502). I have a problem with determining the properties of the ring $R = Z[(1+\sqrt{-19})/2]$. I suppose that it is a UFD and it is not a Euclidean domain. Also, I supose that it is a PID. What could you tell me about it?

Answer: The ring $R = Z[(1+\sqrt{-19})/2]$ is one of the first known examples of a PID that is not a Euclidean domain. Note that the quotient field of $Z[(1+\sqrt{-19})/2]$ is the field $Q(\sqrt{-19})$ which is an example of a quadratic extension $Q(\sqrt{d})$ where d is a squarefree nonzero integer (different from 1). Here are a few notes to ease the reading of the answer.

(I) Each element of $Q(\sqrt{d})$ can be expressed as $x+y\sqrt{d}$ to which we can associate a value called *norm* by $N(x+y\sqrt{d}) = (x+y\sqrt{d})(x-y\sqrt{d}) = x^2-y^2d.$ It is easy to verify that if $u,v \in Q(\sqrt{d})$ then $N(uv) = N(u)N(v).$

(II) Note that every $u = x+y\sqrt{d}$ satisfies a quadratic equation: $(u = x+y\sqrt{d} \Rightarrow u-x = y\sqrt{d} \Rightarrow (u-x)^2 = y^2d \Rightarrow u^2-2ux+x^2-y^2d = 0.$ This is why $Q(\sqrt{d})$ is called a quadratic extension of Q.

(III) If $u = x+y\sqrt{d} \in Q(\sqrt{d})$ is such that $2x$ and x^2-y^2d are both integers (i.e. if u satisfies a monic quadratic equation with integer coefficients) then u is called an algebraic integer of $Q(\sqrt{d})$.

(IV) The set of all algebraic integers of $Q(\sqrt{d})$ is an integral domain. The following theorems are well known.

(1) Let d be a squarefree integer different from 0 and $1.$ The set of all algebraic integers $IQ(\sqrt{d})$of $Q(\sqrt{d})$ is $Z[\sqrt{d}]$ if $d \equiv 2 \bmod 4$ or $d \equiv 3 \bmod 4$ and $IQ(\sqrt{d}) = Z[(1+\sqrt{d})/2]$ if $d \equiv 1 \bmod 4.$

(2) $u \in IQ(\sqrt{d})$ is a unit if and only if $N(u) = 1$ or $-1.$

(V) Of interest is the fact that if $x+y\sqrt{d}$ is an algebraic integer in $Q(\sqrt{d})$ then $N(x+y\sqrt{d})$ is an integer and of course if $d < 0$ as in our case $N(x+y\sqrt{d}) = x^2-y^2d$ is a non-negative integer.

(VI) Indeed if $N(x+y\sqrt{d})$ is a prime then the integer $x+y\sqrt{d}$ is irreducible, because of the fact that $N(uv) = N(u)N(v).$

Now a typical $u \in R = Z[(1+\sqrt{-19})/2]$ can be written as $u = x+y(1+\sqrt{-19})/2,$ which has the standard form in $Q(\sqrt{-19})$ as $u = (x+\frac{y}{2})+y\sqrt{-19}/2.$ So $N(u) = (x+\frac{y}{2})^2+19\frac{y^2}{4} = x^2+xy+5y^2.$ So, $N(u) = 1 \Leftrightarrow u = \pm 1.$

(VII) You also need to know that if a and b are integers with $b > 0$ then we can choose integers q and r such that $a = bq+r$ such that $|r| \leq \frac{b}{2}.$ The idea is simple. By the Euclidean algorithm we have unique Q and R such that $a = bQ+R,\ 0 \leq R < b.$ If $R \leq \frac{b}{2}$ we have nothing more to do. If on the other hand $\frac{b}{2} < R < b$ then subtracting b throughout gives $-\frac{b}{2} < R-b < 0.$ This gives us $|R-b| < \frac{b}{2}.$ Setting $q = Q+1$ and $r = R-b$ we have the required inequality.

Let us first show that R is a principal ideal domain (PID). We shall use Hasse's criterion for PID's for this purpose.

Hasse's Criterion: An integral domain D is a PID if and only if there exists a function $f : D\backslash\{0\} \to N \cup \{0\}$ such that (H_1) $x \mid y$ implies $f(x) \leq f(y)$ with equality if $y \mid x$ also, and (H_2) if $x \nmid y$ and $y \nmid x$ then there exist $z,w,d \in D$ such that $d = zx-wy$ with $f(d) < \min(f(x),f(y)).$

Proposition 1. $R = Z[(1+\sqrt{-19})/2]$ is a PID.

Proof. Note that the norm N satisfies H_1 obviously. This leaves us with the verification of H_2. For this, choose y so that $N(y) \leq N(x)$. (If $N(x) \leq N(y)$ we can write $-d = wy - zx$ and switch x and y.) Note that $0 < N(zx - wy) < N(y)$ if and only if $0 < N(z(\frac{x}{y}) - w) < 1$. Here $\frac{x}{y} \in Q(\sqrt{-19})$ and so we can write $\frac{x}{y} = \frac{a+b\sqrt{-19}}{c}$ where a, b, c are integers and we can assume that $(a,b,c) = 1$. Since $y \nmid x$ we must have $c \neq 1$ and as we can take $c > 0$ we can say that $c > 1$. The idea of the proof is that for each value (≥ 2) of c we can find z and w so that $N(z(\frac{x}{y}) - w) < 1$. To do this we first deal with the case when $c \geq 5$.

Since $(a,b,c) = 1$ we can find d, e, f so that $ae + bd + cf = 1$. Let $ad - 19be = cq + r$ where $|r| \leq \frac{c}{2}$. We show that by choosing $z = d + e\sqrt{-19}$ and $w = q - f\sqrt{-19}$ we have the required result for $c \geq 5$. Substituting these values we have $z(\frac{x}{y}) - w = \frac{(d+e\sqrt{-19})(a+b\sqrt{-19})}{c} - (q - f\sqrt{-19})$ $= \frac{(ad-19be)+(ae+bd)\sqrt{-19}-cq+cf\sqrt{-19}}{c} = \frac{r+(ae+bd+cf)\sqrt{-19}}{c} = \frac{r+\sqrt{-19}}{c} \neq 0$, and $N(\frac{r+\sqrt{-19}}{c}) = \frac{r^2+19}{c^2}$. For $c = 5$, recall that $|r| \leq \frac{c}{2}$, so $r \leq 2$ and $\frac{r^2+19}{c^2} \leq \frac{4+19}{25} < 1$. For the case of $c \geq 6$ using $|r| \leq \frac{c}{2}$ directly we have $N(\frac{r+\sqrt{-19}}{c}) = \frac{r^2+19}{c^2} \leq \frac{1}{4} + \frac{19}{36} < 1$. This leaves us with $c = 2, 3, 4$. We deal with each separately.

(i) $c = 2$. In this case a and b must have different parity and a must be odd. Because a and b being both even contradicts $(a,b,c) = 1$ and a and b being both odd gives $\frac{x}{y} = \frac{a+b\sqrt{-19}}{2} = \frac{a-b+b(1+\sqrt{-19})}{2} \in R$, contradicting $y \nmid x$. Also, a being even puts $\frac{x}{y} = \frac{a+b\sqrt{-19}}{2} \in R$, again contradicting $y \nmid x$. Now let $z = 1$ and $w = \frac{a-1+b\sqrt{-19}}{2}$ which are elements of R. Then $z(\frac{x}{y}) - w = \frac{a+b\sqrt{-19}}{2} - \frac{a-1+b\sqrt{-19}}{2} = \frac{1}{2}$ and $N(\frac{1}{2}) < 1$.

(ii) $c = 3$. If $c = 3$, $(a,b,c) = 1$ implies that $a^2 + 19b^2 \equiv a^2 + b^2 \equiv r \bmod(3)$ where $r = 1, 2$. Set $z = a - b\sqrt{-19}$ and $w = q$ where q comes from $a^2 + 19b^2 = 3q + r$ with $r = 1, 2$. Then, in this case, $z(\frac{x}{y}) - w = (a - b\sqrt{-19})(\frac{a+b\sqrt{-19}}{3}) - q = \frac{a^2+19b^2-3q}{3} = \frac{3q+r-3q}{3} = \frac{r}{3}$ which is nonzero with norm less than 1.

(iii) $c = 4$. In this case a and b are not both even because $(a,b,4) = 1$. If a and b are of opposite parity then since $a^2 + 19b^2 \equiv (a^2 - b^2) \bmod(4)$ we have $a^2 + 19b^2 = 4q + r$ where $0 < r < 4$. Set $z = a - b\sqrt{-19}$ and $w = q$ we have $z(\frac{x}{y}) - w = \frac{a^2+19b^2}{4} - q = \frac{r}{4}$ which is nonzero with norm less than 1. If on the other hand a and b are both odd then $a^2 + 19b^2 \equiv (a^2 + 3b^2) \bmod(8)$ and $(a^2 + 3b^2) \neq 0 \bmod(8)$.

Call a nonzero nonunit d a universal side divisor (usd) of a domain D if for each $x \in D$ there is a $z \in U(D) \cup \{0\}$ such that $d \mid x - z$. (Here $U(D)$ denotes the set of units of D.) Recall also that an integral domain D is a Euclidean domain if there is a function $\varphi : D \backslash \{0\} \to N \cup \{0\}$, let us call φ a norm, such that for all $y \in D \backslash \{0\}$ (i) $\varphi(x) \leq \varphi(xy)$, for all $x \in D \backslash \{0\}$ and (ii) for each pair $x, y \in D \backslash \{0\}$ there are z, w such that $x = yz + w$ where $w = 0$ or $\varphi(w) < \varphi(y)$.

Observation 2. If D is a Euclidean domain that is not a field then D contains a usd for each norm φ, $R = Z[(1+\sqrt{-19})/2]$ does not have a usd and hence is not a Euclidean domain under any norm.

Proof. Let φ be a norm for which D is Euclidean. Then, as D is not a field, D has a non-zero nonunit u with a minimal norm. Now let y be an element of D and write $y = qu + r$ where $r = 0$ or$\varphi(r) < \varphi(u)$. But as $\varphi(u)$ is mimimal we cannot have $\varphi(r) < \varphi(u)$ unless $r = 0$ or a unit and in either case u divides $y - r$. Now we show that $R = Z[(1 + \sqrt{-19})/2]$ cannot have a usd and hence is is not Euclidean.

Note that -1 and 1 are the only units of $R = Z[(1 + \sqrt{-19})/2]$. So the set of zeros and units combined is $\{0, -1, 1\}$. If u is a usd for R then u must divide at least one of $2 \pm 0, 2 \pm 1$, i.e., at least one of $2, 1, 3$. Of these 1 is out because u is not a unit. So, the set from where the universal side divisors can come is $S = \{2, -2, 3, -3\}$. Note that as 2 and 3 are irreducible in the PID R they are primes. Now consider $x = \frac{1+\sqrt{-19}}{2}$. If there is a usd then it must also divide at least one of $T = \{\frac{1+\sqrt{-19}}{2}, \frac{1+\sqrt{-19}}{2} \pm 1\} = \{\frac{1+\sqrt{-19}}{2}, \frac{3+\sqrt{-19}}{2}, \frac{-1+\sqrt{-19}}{2}\}$, but these are all primes because $N(\frac{1+\sqrt{-19}}{2}) = \frac{1+19}{4} = 5$, $N(\frac{3+\sqrt{-19}}{2}) = \frac{9+19}{4} = 7$ and $N(\frac{-1+\sqrt{-19}}{2}) = 5$. So, no member of S divides any member T and hence there is no usd. Since R is a PID and since S and T consist of primes the above argument is norm independent.

Comment: Jim Coykendall provided a rough sketch of the proof of R being non-Euclidean PID. I used the following paper to complete the picture: Jack C. Wilson, "A principal ideal ring that is not a Euclidean ring" Math. Mag. 46 (1973), 34–38. Muhammad Zafrullah