Integers in quadratic fields; EDs and PIDs.

Kevin Buzzard

February 9, 2012

Last modified 06/16/2009.

All rings are commutative and have a 1 in this note. A *Euclidean domain* is an integral domain R for which there exists a function $f : R\backslash\{0\} \to \mathbf{Z}_{\geq 0}$ with the property that for any $a, b \in R$ with $b \neq 0$, we can write $a = qb + r$ with either $r = 0$ or $f(r) < f(b)$. We call any such f a *Euclidean function* on R.

We say that a number field is *Euclidean* if its ring of integers R is an ED. We say it's *norm-Euclidean* if the absolute value of the norm $N_{R/\mathbf{Z}}$ is a Euclidean function on R. Of course, norm-Euclidean implies Euclidean implies PID for integers of number fields, and PID is equivalent to UFD for these rings.

Here are some deeper facts though. Let K be a number field with ring of integers R. Firstly, if K is Galois over $\mathbf{Q}$ and has unit rank greater than 3, then ED and PID are equivalent for R (this is a theorem of Harper and R. Murty from 2004). Furthermore, under GRH, ED and PID are equivalent for any K such that R has infinitely many units (a theorem of Weinberger from 1972)! So to understand the difference between ED and PID we only need to consider the case of imaginary quadratic fields. Another deep theorem gives a complete list of the im quad fields for which R is a PID; they are $\mathbf{Q}(\sqrt{-N})$ for $N \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

Now back to easier facts. Let's consider those nine im quad fields. The first five of these are norm-Euclidean: to verify this it suffices to check that for any $z \in \mathbf{C}$ the distance from z to R is strictly less than 1 (and then we apply this with $z = a/b$ and let q be the nearest element of R). Here's the check explicitly for $N = 11$: if $z = x + iy$ then WLOG $-\sqrt{11}/4 \leq y < \sqrt{11}/4$ (change z to $z - r$ for $r \in R$) and now observe that any such y is within $1 - \epsilon$ of $\mathbf{Z}$ because $\sqrt{11}/4 < \sqrt{3}/2$. Observe also that this argument does not work for $N \geq 19$. Note that this argument won't deal with the last four—but in fact the last four fields aren't even EDs! The proof of this is surprisingly (in my mind) easy: if f is a Euclidean function on R, one of these last four rings, then let n be the minimal value that f takes on $R - \{0, 1, -1\}$ (I'm removing zero and the units) and let b be any element of $R - \{0, 1, -1\}$ with $f(b) = n$. Now for any $a \in R$ we have $a = qb + r$ and either $r = 0$ or $f(r) < f(b) = n$ and hence $r = \pm 1$. Hence $R/(b)$ has at most three elements. But 2 and 3 are both inert in R! (Jan Saxl pointed me to a paper in the AMM containing this argument when I was an undergraduate).

For integers of real quadratic fields we have a bunch of conjectures and some results. Of course it's well-known that they have infinitely many units, so under GRH we should have ED iff PID for integers in real quadratic fields. It's a conjecture that infinitely many are PIDs. The complete list of integers R in quadratic fields $\mathbf{Q}(\sqrt{d})$ which are norm Euclidean is known: it's Sloane A048981 and runs from $d = -11$ to $d = 73$. The first two squarefree positive integers not in the list are 10 (which is not a PID) and 14, which is very interesting! It is a PID but not a norm ED [exercise: check that you can't divide $1 + \sqrt{14}$ by 2, because if a, b are odd and $|a^2 - 14b^2| < 4$ then modulo 8 says $a^2 - 14b^2 = 3$ and 3 is inert in $\mathbf{Z}[\sqrt{14}]$]. More surprisingly, it was only proved to be an ED in 2004! (Harper, Can. J. Math.) The strategy appears to use an observation of Motkin: we showed above that in an ED there must be some $s \in R$, not zero or a unit, with every element of $R/(s)$ represented by 0 or a unit. One can go on from this. One sets $A_0 = \{0\}$, $A_1 = R^\times$, and for $n \geq 2$ let A_n be the $s \in R$ such that the map $\cup_{i<n} A_i \to R/(s)$ is surjective. Then R is an ED *if and only if* R is the union of the A_n. It seems to be a non-trivial theorem then that $\mathbf{Z}[\sqrt{14}]$ is an ED!