EULER'S DESCENT

ISHAN LEVY

Which odd primes are of the form x^2+ny^2? One approach to solve this problem for small n taken by Euler is to split it into two problems, the reciprocity step, or finding when $p|x^2+ny^2, p\nmid x,y$ and the descent step, to take the number that p divides and replace it with p itself. For the reciprocity step, $p|x^2+ny^2 \iff (\frac{-n}{p})=1$, and this can be characterized via Jacobi reciprocity. Supposing we have $p|N=x^2+ny^2$, we can always choose $|x|,|y|<p/2,(x,y)=1$, so that $N<(1+n)(\frac{p^2}{4})$. If $n\leq 3$, all other factors of N have to be smaller than p.

Now the main lemma is that if $N\in\mathbb{Z}$ and $q\in\operatorname{Spec}(\mathbb{Z})$ are of the form a^2+nb^2 for relatively prime a,b, then N/q is too. From this, we can either continue to get smaller N that p divides until $p=N$, or find a smaller prime not of the form a^2+nb^2. By Fermat descent this is impossible (for n=3 one has to be make sure that the descending sequence of primes is odd).

So we are left to prove the main lemma, which holds for any n.

Lemma 0.1. *If $N\in\mathbb{Z}$ is of the form a^2+nb^2 and $q\in\operatorname{Spec}(\mathbb{Z})$ is of the form x^2+ny^2 and $q|N, q\nmid n$, then $N/q=c^2+nd^2$. Moreover, if $(a,b)=1$, $(c,d)=1$.*

Proof. The key to proving this will be two view it as a partial converse to the fact that

$$(x^2+ny^2)(c^2+nd^2)=(xc-nyd)^2+n(xd+yc)^2$$

To get the result, we will try to reconstruct c,d from the data a,b,x,y,q,N, using the fact that q is prime. To use this fact, we will need q to divide something that factors, namely, $Nx^2-qa^2=n(xb-ya)(xb+ya)$. By possibly changing the sign of a, we can assume $q|xb-ya$. But note that $xb-ya=dq$ in the equation above, so we can call define d according to the main equation above. Similarly, $q|Nx^2-nqb^2=(ax+nby)(ax-nby)$ so after a change of sign $q|ax+nby=qc$, so we can recover c. To check that this is sufficient, we calculate

$$q(c^2+nd^2)=\frac{(ax+nby)^2+n(xb-ya)^2}{q}=\frac{Nq}{q}=N$$

Finally if we can show that actually $a=xc-nyd, b=xd+yc$, it will be shown that $(c,d)=1$ if $(a,b)=1$. To do this, we can recover c in a different way. Namely

Date: June 2, 2020.

we can try to show that $x|a + nyd = xc$, and since $(x, y) = 1$, this is equivalent to $x|ay + ny^2d = bx - dx^2$, so we can define c this way. Then the main equation still holds. $\square$

Remark: the condition $q \nmid n$ has to do with ramification in the ring $\mathbb{Z}[\sqrt{-n}]$.

Remark: We should not expect in general for it to be the case that $p|a^2 + nb^2 \implies p = a^2 + nb^2$. For example, $2|1^2 + 5 * 1^2$, but 2 is not of the desired form. This can be explained by the fact that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Indeed $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\sqrt{-3}]$ are UFDs away from the prime 2 so, from a more modern point of view we can see why this argument only works for small n.