Klaus Hoechsmann, UBC.

EUCLID WITHOUT HURWITZ.

Let $\mathcal{Z} \subset \mathcal{Q}$ denote the quaternions with integral and rational coefficients, respectively, and consider the element $\rho \in \mathcal{Q}$ defined by $2\rho = 1 + i + j + k$. The vertices of the unit cube W with center 0 are precisely the points $u\rho$ and $u\bar{\rho}$, where u denotes any of the 8 units ± 1, $\pm i$, $\pm j$, $\pm k$ of the ring $\mathcal{Z}$. As $\rho\bar{\rho} = \rho + \bar{\rho} = 1$, it is clear that $\rho^3 = -1$. The ring $\mathcal{H} = \mathcal{Z}[\rho]$ consists of all $\lambda \in \mathcal{Q}$ such that $\lambda + \bar{\lambda}$ and $\lambda\bar{\lambda}$ are integers. Sometimes called the ring of *Hurwitz* quaternions, $\mathcal{H}$ forms the customary arithmetic arena within $\mathcal{Q}$. Our aim is to show that Euclid's algorithm also works quite well in $\mathcal{Z}$ itself.

Obviously every $\mu \in \mathcal{Q}$ is of the form $z + \varepsilon$, where $z \in \mathcal{Z}$ and $\varepsilon \in W$, so that $|\varepsilon| \leq 1$ with equality iff ε is a vertex of W. Given non-zero elements $n, m \in \mathcal{Z}$, we apply this to $\mu = nm^{-1}$ and get

$$n = zm + r \;, \qquad z, r \in \mathcal{Z}, \qquad |r| \leq |m|, \tag{$*$}$$

with equality iff $r = \varepsilon m$, where ε is a vertex of W. To find a criterion for the occurrence of equality, consider the ring homomorphism $s : \mathcal{Z} \longrightarrow \mathbb{F}_2$ given by

$$s : \; a + bi + cj + dk \longmapsto a + b + c + d \pmod 2.$$

Note that the quaternions over $\mathbb{F}_2$ form the group algebra $\mathbb{F}_2 V$ of the Klein four-group V, and s is just the augmentation map.

Lemma: *Let ε be a vertex of W, and $m \in \mathcal{Z}$. Then $\varepsilon m \in \mathcal{Z}$ if and only if $s(m) = 0$, in which case $\alpha m \in \mathcal{Z}$ and $s(\alpha m) = 0$ for all vertices α of W.*

Proof: Consider the element $e = 2\varepsilon$ in $\mathcal{Z}$. Obviously $\varepsilon m \in \mathcal{Z}$ if and only if $em \in 2\mathcal{Z}$, i.e., $em = 0 \in \mathbb{F}_2 V$. However, in $\mathbb{F}_2 V$ every 2α looks like $1 + i + j + k$, and $em = s(m)e$.

Theorem: *If $\mathcal{L}$ is a non-principal left ideal of $\mathcal{Z}$, then $s(\mathcal{L}) = 0$ and $\mathcal{L}$ has two generators g, ρg or three generators g, ρg, $\bar{\rho} g$.*

Proof: Let $m \in \mathcal{L}$ have minimal positive norm. Applying $(*)$ to any $n \in \mathcal{L}$, we might always find $r = 0$, and then $\mathcal{L}$ is principal. Otherwise we obtain $n = zm + \varepsilon m$ at some point. By the lemma, it then follows that $s(m) = 0$ and that $\alpha m \in \mathcal{Z}$ for all vertices α of W. Clearly $\mathcal{L}$ is generated by m and a non-empty subset of the αm, and therefore $s(\mathcal{L}) = 0$. Finally, since every vertex of W can be written as $u\rho$ or $u\bar{\rho}$ with $u \in \mathcal{Z}^\times$, the theorem follows.

Remark: Obviously every $\mathcal{L}$ becomes principal in $\mathcal{H}$. In trying to express an odd natural prime p as a sum of four squares, one applies the Euclidean algorithm to the ideal $\mathcal{L} = \mathcal{Z}p + \mathcal{Z}m$, where $m\bar{m} \equiv 0 \pmod p$. Since $s(p) \neq 0$ in $\mathbb{F}_2$, this ideal is always principal.