AC, 15^{th} December 2008

M3P14 Elementary Number Theory—Problem Sheet 5.

(1) Let R be the set of numbers of the form

$$a + bi\sqrt{5}$$

where a, b are integers.
(a) Verify that R is a ring (don't fret too much over this).
(b) Show that the only solutions of $\alpha\beta = 1$ in R are $\alpha = \beta = 1$ and $\alpha = \beta = -1$, that is, ± 1 are the only units in R.
(c) Show that $3 + 2i\sqrt{5}$ divides $85 - 11i\sqrt{5}$ in R.
(d) Show that the number 2 is irreducible in R.
(e) Define the norm $N(a+bi\sqrt{5}) = a^2+5b^2$. Let $\alpha = 11+2i\sqrt{5}$ and $\beta = 1+i\sqrt{5}$; show that it is not possible to find elements γ and ρ in R such that

$$\alpha = \beta\gamma + \rho \quad \text{and} \quad N(\rho) < N(\beta).$$

(f) The irreducible 2 divides the product

$$(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6$$

but it does not divide any of its factors; in other words the irreducible 2 is not prime.
(g) Show that the number 6 has two distinct factorisations into irreducibles of R:

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

(2) It's a theorem that a non-negative integer can be written as the sum of three squares if and only if the integer is not of the form $4^t(8n + 7)$ for $t, n \geq 0$. Prove the easier implication: That is, show that integers of the form $4^t(8n + 7)$ are never the sums of three squares.

(3) In this question, denote by

$$\mathcal{O} = \mathbb{Z}[i, j, k] + \mathbb{Z}\frac{1 + i + j + k}{2}$$

the (non-commutative) ring of *integer quaternions*, sometimes also called *Hurwitz quaternions* (in this ring, $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$).
(a) Show that the group of unit Hurwitz quaternions, that is, the group of $u \in \mathcal{O}$ such that there exists $v \in \mathcal{O}$ with $uv = 1$, is the (non-commutative) group:

$$\mathcal{O}^\times = \left\{\pm 1, \pm i, \pm j, \pm k, \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k\right\}$$

Show that this is the same as the group of Hurwitz quaternions of norm 1.
(b) Show that $\mathcal{O}$ is both right and left Euclidean, that is, for all $\alpha, \beta \in \mathcal{O}$ with $\beta \neq 0$, there exist γ, ρ and $\gamma', \rho' \in R$ such that

$$\begin{aligned} \alpha &= \beta\gamma + \rho \quad \text{with} \quad N(\rho) < N(\beta), \\ \alpha &= \gamma'\beta + \rho' \quad \text{with} \quad N(\rho') < N(\beta). \end{aligned}$$

(c) Show that, by contrast, the ring $\mathbb{Z}[i,j,k]$ is *not* Euclidean: indeed, show that it is impossible to 'divide' $1+i+j+k$ by 2 (either from the right or from the left, it doesn't matter) and obtain a remainder of norm < 4.

(d) Use (b) to show carefully that there is in $\mathcal{O}$ a 'right' hcf, in other words: Given $\alpha, \beta \in \mathcal{O}$, with $\beta \neq 0$, there exists a Hurwitz quaternion

$$\gamma = \mathrm{hcf}^R(\alpha, \beta)$$

that satisfies the following two properties:

(i) $\alpha = \alpha'\gamma$, $\beta = \beta'\gamma$ for some Hurwitz quaternions $\alpha', \beta' \in \mathcal{O}$—that is to say, γ divides α and β *from the right*;

(ii) There exist Hurwitz quaternions $\xi, \eta \in \mathcal{O}$ such that

$$\xi\alpha + \eta\beta = \gamma.$$

Prove that properties (i) and (ii) characterize γ upto *left* multiplication by a unit: if γ' satisfies (i) and (ii), then $\gamma = u\gamma'$ for some unit $u \in \mathcal{O}^\times$.

Show that this is not the same as right multiplication by a unit: produce Hurwitz quaternions γ, γ' such that $\gamma = u\gamma'$ for some unit $u \in \mathcal{O}^\times$, but there is no unit $w \in \mathcal{O}^\times$ such that $\gamma = \gamma' w$.

(e) Briefly make a similar statement regarding a left hcf.

(4) Find a polynomial with integer coefficients that has the number $\sqrt{2} + \sqrt[3]{3}$ as one of its roots. Do the same with the number $\sqrt{5} + i$.

(5) Set $r = 2^{1/3}$.
(a) Prove that r is algebraic but not rational.
(b) (a little tricky if you've not seen this kind of thing before) Prove that f is algebraic of degree 3.
(c) (if you didn't do (b) then just assume it). Run through the proof of Liouville's theorem and find an explicit constant $c > 0$ such that for all rationals p/q with $p, q \in \mathbb{Z}$ and $q > 0$, we have $|r - p/q| > c/q^3$.

(6) Prove that $\sum_{n \geq 1} 2^{-(2^{2^n})}$ is transcendental.