Mathematics 676-4 **Homework (due Apr. 2)** A. Hulpke

32) Write $\frac{8}{15}$ as a 2-adic number and as a 5-adic number.

33) Let P be a set of positive prime numbers. Define

$$O_P := \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, 0 \neq b \in \mathbb{N}; p \not| b \text{ for all } p \in P \right\},$$

then O_P is a ring (you do not need to show this). Describe the ideals of O_P. What can one conclude from this about the subrings of $\mathbb{Q}$, containing $\mathbb{Z}$?

34*) Let p be a prime. Show that $\mathbb{Z}_p$, the ring of p-adic integers contains the $(p-1)$-first roots of unity.
Hint: For $a \in \mathbb{Z}$ with $- \leq a \leq p-1$ consider a sequence $\left(a^{p^n}\right)_{n\in\mathbb{N}}$. To show that it is a Cauchy sequence, it is sufficient (because the valuation is nonarchimedic!) to show that the valuation of differences converges to 0.

35) In this problem we want to derive a p-adic method for solving systems of integral equations which is due to JOHN DIXON and RICHARD PARKER:
Let $\underline{\mathbf{a}}_1, \ldots, \underline{\mathbf{a}}_m \in \mathbb{Z}^n$ vectors that are $\mathbb{Z}$ linear independent and let $b \in \mathbb{Z}^n$ in the $\mathbb{Z}$-Span of these vectors. We want to solve $A\underline{\mathbf{x}} = \underline{\mathbf{b}}$ with $\underline{\mathbf{x}} \in \mathbb{Z}^n$, where A is the matrix given by the coefficients of the $\underline{\mathbf{a}}_i$.
a) For which primes does the system $A\underline{\mathbf{x}} = \underline{\mathbf{b}}$ have a unique solution?
b) Given a solution $\underline{\mathbf{x}}_1$ so that $A\underline{\mathbf{x}}_1 \equiv \underline{\mathbf{b}} \pmod{p^a}$, show how to modify $\underline{\mathbf{x}}_1$ to obtain a solution $\underline{\mathbf{x}}_2$ so that $A\underline{\mathbf{x}}_2 \equiv \underline{\mathbf{b}} \pmod{p^{(a+1)}}$.
c) Use this method to find an integer solution to the system

$$\begin{pmatrix} 12 & 34 & 23 \\ 34 & 17 & 18 \\ 3 & 18 & 19 \end{pmatrix} \cdot \underline{\mathbf{x}} = \begin{pmatrix} 3815 \\ 4345 \\ 2450 \end{pmatrix}$$

36*) Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n and $\alpha \in \bar{\mathbb{Q}}$ with $f(\alpha) = 0$. Let g be the minimal polynomial of α.
a) Show that $g \in \mathbb{Z}[x]$.
b) Let N be the nullspace of the matrix $(1, \alpha, \alpha^2, \ldots, \alpha^n)$. Show, that the coefficient vector of g is an element of N.
c) Suppose α is given approximatively by a (floating point or p-adic) number β. Let $\mathcal{B}$ be a basis of the nullspace of $(1, \beta, \beta^2, \ldots, \beta^n)$, consisting of integer vectors (for example obtained by scalar multiplication and rounding). Show, that for a sufficiently good approximation of β the coefficient vector of g lies in the $\mathbb{Z}$-span of $\mathcal{B}$ (this span is a lattice).
d) Let $\mathcal{B}$ as in part c). Show that for a suitable (weighted) norm on $\mathbb{R}^{n+1}$ the coefficients of g form a shortest vector in the lattice spanned by $\mathcal{B}$.
e) Assuming a method to find the shortest vectors in a lattice, describe a method to factor a polynomial $f \in \mathbb{Z}[x]$ into irreducible factors, based on computing minimal polynomials of roots.

Problems marked with *are bonus problems for extra credit.

I will be at a conference out of town between 3/22 and 3/29.