36*) Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n and $\alpha \in \overline{\mathbb{Q}}$ 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.

37) Compute a reduced basis for the lattice spanned by the rows of the matrix

$$\begin{pmatrix} 787 & 843 & -533 \\ -1910 & -2045 & 1294 \\ -220 & -236 & 147 \end{pmatrix}$$

Compare your result with that obtained by "proper" LLL reduction, using the GAP command `LLLReducedBasis`.

38) Let S be a positive definite symmetric bilinear form on R^n (with a corresponding norm $\|a\|_S = \sqrt{S(a,a)}$. We want to find vectors in $\mathbb{Z}^n \subset \mathbb{R}^n$ that are short with respect to **this** norm (and not necessarily with respect to $\|\cdot\|_2$).
a) Show that there is a linear transformation $\varphi: R^n \to R^n$, such that $\|a\|_S = \|\varphi(a)\|_2$.
b) Show that $L = \{\varphi(l) \mid l \in \mathbb{Z}^n\}$ is a lattice in R^n and that short vectors in L with respect to $\|\cdot\|_2$ correspond to short vectors in $\mathbb{Z}^n$ with respect to $\|\cdot\|_S$.
c) Find vectors in $\mathbb{Z}^3$ that are short with respect to the scalar product

$$S(\underline{\mathbf{x}}, \underline{\mathbf{y}}) = \underline{\mathbf{x}}^T A \underline{\mathbf{y}} \quad \text{with} \quad A = \begin{pmatrix} 9 & 15 & -6 \\ 15 & 41 & 46 \\ -6 & 46 & 209 \end{pmatrix}$$

39) a) Let S be a positive definite symmetric bilinear form on R^n, given by (as in problem 38) the matrix A (this matrix is called the Gram matrix for S with respect to the standard basis). . Let $C \in \mathbb{R}$. Show that there are bounds $c_i = c_i(C)$ (depending on A and C) so that if $\underline{\mathbf{x}} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ with $S(\underline{\mathbf{x}}, \underline{\mathbf{x}}) = \underline{\mathbf{x}}^T A \underline{\mathbf{x}} \leq C$, then $|x_i| \leq c_i$.
b) Let $\mathcal{B}$ be another $\mathbb{Z}$-basis of the lattice Z^n gigven by the columns of the matrix $B \in \mathbb{Z}^{n \times n}$. Let $D = B^T \cdot A \cdot B$ the matrix for the form S with respect to the basis B. Show that it is also possible to compute the shortest vectors using the basis $\mathcal{B}$ and the matrix D instead.
c) Let

$$A = \begin{pmatrix} 44 & -2 & -16 \\ -5 & 6 & 0 \\ -15 & -1 & 6 \end{pmatrix}.$$

Determine all vectors in $\mathbb{Z}^n$ with $S(\underline{\mathbf{x}}, \underline{\mathbf{x}}) \leq 3$.
Note The `.remainder` component of the result of `LLLReducedGramMat` (see the online help or the manual) contains the Gram matrix for S with respect to a basis reduced with respect to S. By b) one can work in this new basis.

40) Find a combination of the numbers

$$276, 1768, 1993, 2536, 4251, 4884, 5020, 5347, 7401, 9072$$

That sums up to 33164.
Hint: The command

```
m:=IdentityMat(11,1);;m{[1..11]}[11]:=l;
```

creates an identity matrix whose 11th column in rows $1 \ldots 10$ contains the values in the list `l`.

Problems marked with *are bonus problems for extra credit.

From April 7 on, we will also meet Mondays, at 9am in Engineering B103 to make up for lost lectures.