2 Elimination over the Integers

How to solve systems of linear equations over the ring $\mathbb{Z}$ of integers? How to calculate determinants efficiently? How to find an inverse matrix? Like in linear algebra over fields also in the more general situation over rings the *triangularization* of matrices is crucial for finding efficient algorithms.

For a sufficiently general framework we consider three classes of rings (commutative, with 1, without zero divisors):

- **Factorial rings** (or UFD domains): All elements have a decomposition into primes, in particular any two elements have a greatest common divisor gcd (in general not unique).
- **Principal ideal domains:** Each ideal is a principal ideal. Principal ideal domains are factorial, and the gcd of any two elements is a linear combination of these two.
- **Euclidean rings:** They have a division with remainder. Euclidean rings are principal ideal domains. The gcd of two elements as well as its linear represenation can be efficiently calculated by the extended Euclidean algorithm.

The set of invertible matrices with determinant 1 over a ring is called the "special linear group" $SL_n(R) \subseteq GL_n(R)$. It is the kernel of the determinant homomorphism on $GL_n(R)$.

Lemma 1 *Let R be a principal ideal domain, $a_1, \ldots, a_n \in R$, and d a $\gcd(a_1, \ldots, a_n)$. Then there is an invertible matrix $U \in SL_n(R)$ such that*

$$U \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Proof. Since the case $n = 1$ is trivial we may assume $n \geq 2$.

If all $a_i = 0$, then the assertion is trivial. Otherwise we may assume without restriction that $a_1 \neq 0$ (after a permutation that is merged into U as permutation matrix—if necessary replace a 1 by -1 to make the determinant $= 1$).

Let $d_2 := \gcd(a_1, a_2)$ (*any* gcd because in general this is not unique). Then $d_2 \neq 0$ and $d_2 = c_1 a_1 + c_2 a_2$ is a linear combination. From this we get the equation

$$\begin{pmatrix} c_1 & c_2 \\ -\frac{a_2}{d_2} & \frac{a_1}{d_2} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} c_1 a_1 + c_2 a_2 \\ -\frac{a_2 a_1}{d_2} + \frac{a_1 a_2}{d_2} \end{pmatrix} = \begin{pmatrix} d_2 \\ 0 \end{pmatrix}$$

where the matrix of coefficients

$$C = \begin{pmatrix} c_1 & c_2 \\ -\frac{a_2}{d_2} & \frac{a_1}{d_2} \end{pmatrix} \quad \text{has } \operatorname{Det} C = \frac{c_1 a_1}{d_2} + \frac{c_2 a_2}{d_2} = 1$$

and therefore is invertible.

We proceed be induction: Assume for the general step that for some $i \geq 2$

$$U' \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d' \\ 0 \\ \vdots \\ 0 \\ a_i \\ \vdots \\ a_n \end{pmatrix} \qquad \text{where } a_i \neq 0$$

Then as before we change two coordinates:

$$\begin{pmatrix} d' \\ a_i \end{pmatrix} \rightsquigarrow \begin{pmatrix} d'' \\ 0 \end{pmatrix}.$$

In this way we successively build the matrix U. $\diamond$

Remark The inverse of the matrix C in the proof is

$$C^{-1} = \begin{pmatrix} \frac{a_1}{d_2} & -c_2 \\ \frac{a_2}{d_2} & c_1 \end{pmatrix}$$

From this formula we see that U and U^{-1} together can be calculated by at most $n-1$ executions of the Euclidean algorithm, plus $n-1$ multiplications of $n \times n$-matrices plus at most $n-1$ multiplications of permutation matrices.

With the help of this lemma we can triangularise matrices. (A more refined analysis would lead to the HERMITEan normal form.)

Theorem 1 (i) *Let R be a principal ideal domain, and $A \in M_{pq}(R)$. Then there exists an invertible matrix $U \in SL_p(R)$ such that $H = UA$ has the form*

$$\begin{pmatrix} * & \dots & * \\ & \ddots & \vdots \\ & & * \\ 0 & & \end{pmatrix} \quad \textit{für } p \geq q, \qquad \begin{pmatrix} * & \dots & \dots & * \\ & \ddots & \dots & \\ 0 & & * & \end{pmatrix} \quad \textit{für } p < q.$$

(ii) *If R is Euclidean, then U and U^{-1} together can be calculated by at most $\frac{p(p-1)}{2}$ executions of the extended Euclidean algorithm.*

Special case Let $A \in M_{pp}(R)$ be a square matrix, and determine $H = UA$ as in the Theorem. Then

$$\operatorname{Det} A = \operatorname{Det} H = h_{11} \cdots h_{pp}.$$

If A is invertible, then $A^{-1} = (U^{-1}H)^{-1} = H^{-1}U$. The calculation of the inverse H^{-1} of the triangular matrix H is easy. Thus calculation of determinant and inverse are reduced to triangularisation.

Proof. We prove this by describing an algorithm. Let $r := \min\{p, q\}$. Initialize the algorithm by

$$H := A, \quad U := \mathbf{1}_p, \quad V := \mathbf{1}_p.$$

Then loop over $j = 1, \ldots r$. The relations $UA = H$, $UV = \mathbf{1}_p$ are loop invariants.

- Assume that at the beginning of the j-th step H has the form:

$$\begin{pmatrix} * & & & & \\ & \ddots & & & * \\ & & * & & \\ & & & h_{jj} & \\ & 0 & & \vdots & \\ & & & h_{pj} & \end{pmatrix}$$

If $h_{jj} = \ldots = h_{pj} = 0$ we finish step j. Otherwise we use the lemma and find a matrix $U' \in SL_{p-j+1}(R)$ together with its inverse $(U')^{-1}$ such that

$$U' \begin{pmatrix} h_{jj} \\ \ldots \\ h_{pj} \end{pmatrix} = \begin{pmatrix} d_j \\ 0 \\ \ldots \\ 0 \end{pmatrix}$$

We have $\left(\begin{smallmatrix} \mathbf{1} & 0 \\ 0 & U' \end{smallmatrix}\right) \in SL_p(R)$. At the end of the loop we replace

$$U := \begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} U, \quad H := \begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} H, \quad V := V \begin{pmatrix} \mathbf{1} & 0 \\ 0 & (U')^{-1} \end{pmatrix}.$$

After finishing the last loop U and H have the desired form. $\diamond$

Summarizing the expenses we have to add $\frac{p(p-1)}{2}$ matrix multiplications and the same number of multiplications by permutation matrices. However the total expenses are not yet covered because bounds for the intermediate results are yet missing. More exact considerations give expenses of the order $\mathrm{O}(m^2n^5)$ where m is an upper bound for the number of digits of the entries of A and $n = \max(p, q)$. For further optimizations of this bound search the literature on algebraic algorithms.

Elimination in Residue Class Rings

Now how to invert a matrix $A \in GL_q(\mathbb{Z}/n\mathbb{Z})$? First interpret A as an integer matrix and determine $U \in SL_q(\mathbb{Z})$ such that $H = UA$ is an integer upper triangular matrix as in Theorem 1. Reduction $\bmod n$ conserves the equation $H = UA$ as well as $A^{-1} = H^{-1}U$. Since $A \bmod n$ is invertible all diagonal elements of H are invertible $\bmod n$.