LMS J. Comput. Math. 17 (Special issue A) (2014) 349–365
doi:10.1112/S1461157014000291

Computing in quotients of rings of integers

Claus Fieker and Tommy Hofmann

Abstract

We develop algorithms to turn quotients of rings of integers into effective Euclidean rings by giving polynomial algorithms for all fundamental ring operations. In addition, we study normal forms for modules over such rings and their behavior under certain quotients. We illustrate the power of our ideas in a new modular normal form algorithm for modules over rings of integers, vastly outperforming classical algorithms.

1. *Introduction*

Rings of integers of number fields are fundamental rings in computational number theory. Similar to algorithms over the integers, a common computational tool is the transfer to quotient rings. This is for example done to prevent intermediate coefficient explosion (Hermite form), allow techniques based on the Chinese remainder theorem (CRT) (utilize the field structure of suitable quotients) or limit the precision in p-adic computations. For quotients $\mathbf{Z}/N\mathbf{Z}$, $N \neq 0$, of $\mathbf{Z}$, the rational integers, this has a rich history, in particular normal forms for matrices or modules over quotients have been studied extensively, both in their own right and as a means to classify matrices and modules over $\mathbf{Z}$ itself. An important observation was the fact that $\mathbf{Z}/N\mathbf{Z}$ can be given the structure of a Euclidean ring, thus allowing the use of general algorithms designed for this class of rings. In contrast to this situation, in rings of integers of number fields, the only properties of quotient rings that have been exploited so far are the fact that residue class rings of prime ideals are fields (CRT based algorithms) and the obvious fact that quotient rings are finite, and thus can be used to avoid intermediate coefficient swell (by reducing modulo some ideal every now and then). However, the algorithms, for example, the modular pseudo Hermite normal form of Cohen [7], or Biasse–Fieker [3], only add the reduction at crucial steps while still basically maintaining the old, underlying, non-modular algorithm.

In this paper, we revive the fact that quotient rings of rings of integers are in fact Euclidean rings allowing for efficient operations. As a result, over such quotient rings, we can immediately use the rich history of algorithms for Euclidean rings. In particular, that allows a much wider class of quotients to be used for non-trivial computations than just the residue class fields. In fact, a short study will immediately show that, since deterministic polynomial factorization over finite fields is very slow, this gives rise to deterministic algorithms for the computation of, say, determinants, of much better complexity.

We illustrate our new ideas by giving a new, truly modular, algorithm for the computation of normal forms over rings of integers. Our algorithm, by utilizing the Euclidean structure of suitable quotients, does not need the complicated (and slow) operations of pseudomatrices and ideals necessary in the classical approach. In fact, for random matrices over rings of integers, the new algorithm has a much better expected runtime than the $\mathbf{Z}$ algorithms on the corresponding $\mathbf{Z}$-module.

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11Y40 (primary), 11-04 (secondary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

Part of this work was supported through the DFG priority programme SPP 1489.

Starting with the Euclidean structure of quotient rings, we then study matrix normal forms under projections before applying everything to matrix normal forms over rings of integers.

2. *Background*

For the rest of the paper we fix an algebraic number field K of degree d with ring of integers $\mathcal{O}$. If $\mathfrak{m}$ is a non-trivial ideal of $\mathcal{O}$, we denote by $\mathbf{N}(\mathfrak{m})$ the ideal norm of $\mathfrak{m}$, that is, $\mathbf{N}(\mathfrak{m}) = |\mathcal{O}/\mathfrak{m}|$. The main goal of this section is the description of the Euclidean structure of $(\mathcal{O}/\mathfrak{m})$, where $\mathfrak{m}$ is a non-trivial ideal of $\mathcal{O}$, based on [10]. The first step consists of defining the Euclidean structure in the case when $\mathfrak{m}$ is a prime ideal power $\mathfrak{p}^l$, exploiting the special properties of the ring $(\mathcal{O}/\mathfrak{p}^l)$. Finally a CRT based procedure is applied to obtain a Euclidean structure on the whole of $(\mathcal{O}/\mathfrak{m})$ for arbitrary $\mathfrak{m}$.

Recall that a commutative ring R is called *Euclidean* if there exists a function $\varphi\colon R\setminus\{0\} \to \mathbf{Z}_{\geqslant 0}$ satisfying the following property: for all $a, b \in R, b \neq 0$ there exist $q, r \in R$ such that

$$a = qb + r \quad \text{with } \varphi(r) < \varphi(b) \quad \text{or } r = 0. \tag{2.1}$$

In this case φ is called a *Euclidean function* and (2.1) is called *Euclidean division*. Note that this is not *the* definition of Euclidean rings but one that suits our purpose. We refer the interested reader to [1] for an overview of possible definitions and relations between them.

Beginning with a prime ideal power $\mathfrak{p}^l$ of $\mathcal{O}$, let us recall some facts about $(\mathcal{O}/\mathfrak{p}^l)$. Let π be an element of $\mathfrak{p}\setminus\mathfrak{p}^2$, the set of $\mathfrak{p}$-uniformizers. Then $(\mathcal{O}/\mathfrak{p}^l)$ is a special principal ideal ring, that is, a ring with unique maximal ideal which is nilpotent, and every ideal is of the form $(\overline{\pi}^k)$ with $0 \leqslant k < l$.

Fixing a set S of coset representatives of $\mathcal{O}$ modulo $\mathfrak{p}$ it is well known that every element $\overline{a}$ of $(\mathcal{O}/\mathfrak{p}^l)$ can be uniquely written in the form

$$\overline{a} = \sum_{i=v_{\mathfrak{p}}(a)}^{l-1} \overline{s}_i \overline{\pi}^i$$

with $s_i \in S$. Moreover $\overline{a}$ is invertible if and only if s_0 is a unit modulo $\mathfrak{p}$. Using this representation it is easy to compute the cardinality of various objects.

LEMMA 1. *We have the following*:
(i) $|(\mathcal{O}/\mathfrak{p}^l)^\times| = \mathbf{N}(\mathfrak{p})^{l-1}(\mathbf{N}(\mathfrak{p}) - 1)$;
(ii) $|(\overline{\pi}^k)| = \mathbf{N}(\mathfrak{p})^{l-k}$ *for* $0 \leqslant k < l$;
(iii) *if* $\mathfrak{a}$ *is an ideal of* $\mathcal{O}$, *then* $\overline{\mathfrak{a}} = (\overline{\pi}^{\min(v_{\mathfrak{p}}(\mathfrak{a}),l)})$ *and* $|\overline{\mathfrak{a}}| = \mathbf{N}(\mathfrak{p})^{l-\min(v_{\mathfrak{p}}(\mathfrak{a}),l)}$;
(iv) *the number of generators of* $(\overline{\pi}^k)$ *is* $\mathbf{N}(\mathfrak{p})^{l-k-1}(\mathbf{N}(\mathfrak{p}) - 1)$ *if* $0 \leqslant k < l$ *and* 1 *if* $k \geqslant l$.

By [10, Proposition 7] the function $(\mathcal{O}/\mathfrak{p}^l)\setminus\{\overline{0}\} \to \mathbf{Z}_{\geqslant 0}, \overline{a} \mapsto v_{\mathfrak{p}}(a)$ defines a Euclidean function on $(\mathcal{O}/\mathfrak{p}^l)$. For the sake of completeness we sketch the argument. The above representation of elements of $(\mathcal{O}/\mathfrak{p}^l)$ shows that every element $\overline{a}$ can be written as $u_a\overline{\pi}^k$ for some unit u_a and unique integer k (in fact $k = v_{\mathfrak{p}}(a)$). If $\overline{a}$ and $\overline{b}$ are elements of $(\mathcal{O}/\mathfrak{p}^l)$ with $\overline{b} \neq \overline{0}$, then

$$\overline{a} = \begin{cases} \overline{0}\cdot\overline{b} + \overline{a}, & \text{if } v_{\mathfrak{p}}(a) < v_{\mathfrak{p}}(b), \\ \overline{u}_a\overline{u}_b^{-1}\overline{\pi}^{v_{\mathfrak{p}}(a)-v_{\mathfrak{p}}(b)}\cdot\overline{b} + \overline{0}, & \text{if } v_{\mathfrak{p}}(a) \geqslant v_{\mathfrak{p}}(b), \end{cases}$$

is a Euclidean division. Composing this Euclidean function with the monotone increasing function $x \mapsto \mathbf{N}(\mathfrak{p})^x$ yields

$$\varphi_{\mathfrak{p}}\colon (\mathcal{O}/\mathfrak{p}^l)\setminus\{\overline{0}\} \longrightarrow \mathbf{Z}_{\geqslant 0}, \quad \overline{a} \longmapsto \mathbf{N}(\mathfrak{p})^{v_{\mathfrak{p}}(a)},$$

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

also turning $(\mathcal{O}/\mathfrak{p}^l)$ into a Euclidean ring. Moreover we extend the function to the whole of $(\mathcal{O}/\mathfrak{p}^l)$ by setting $\varphi_\mathfrak{p}(\overline{0}) = \mathbf{N}(\mathfrak{p})^l$, such that $\varphi_\mathfrak{p}(\overline{a}) = \mathbf{N}(\mathfrak{p})^{\min(v_\mathfrak{p}(a),l)}$ for all $\overline{a} \in (\mathcal{O}/\mathfrak{p}^l)$.

Now we can put everything together. For each prime divisor $\mathfrak{p}$ of $\mathfrak{m}$ denote by $\varphi_\mathfrak{p}\colon (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}) \to \mathbf{Z}$ the Euclidean function defined in the previous paragraph and by $\overline{a}_\mathfrak{p} \in (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})$ the $\mathfrak{p}$-component of an element $\overline{a} \in (\mathcal{O}/\mathfrak{m})$ under the natural isomorphism $(\mathcal{O}/\mathfrak{m}) \cong \prod_{\mathfrak{p}|\mathfrak{m}} (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})$.

PROPOSITION 2. *The ring $(\mathcal{O}/\mathfrak{m})$ together with*

$$\varphi\colon (\mathcal{O}/\mathfrak{m}) \setminus \{\overline{0}\} \longrightarrow \mathbf{Z}_{\geqslant 0}, \quad \overline{a} \longmapsto \mathbf{N}(a, \mathfrak{m})$$

is a Euclidean ring.

Proof. The proof of [10, Proposition 6] shows that $(\mathcal{O}/\mathfrak{m})$ is a Euclidean ring with Euclidean function $\sum_\mathfrak{p} \varphi_\mathfrak{p}(\overline{a}_\mathfrak{p})$. But it is easy to see that the proof remains valid if the sum is replaced by $f((\varphi_\mathfrak{p}(\overline{a}_\mathfrak{p}))_\mathfrak{p})$, where $f\colon \prod_{\mathfrak{p}|\mathfrak{m}} \mathbf{R} \to \mathbf{R}$ is any monotonic multivariate function. The result then follows by choosing f to be the product and noting that $\mathbf{N}(a, \mathfrak{m}) = \varphi(\overline{a}) = \prod_\mathfrak{p} \varphi_\mathfrak{p}(\overline{a}_\mathfrak{p})$. □

We end this section with some remarks on division in $(\mathcal{O}/\mathfrak{m})$. First note that due to the presence of zero-divisors the division in $(\mathcal{O}/\mathfrak{m})$ is not unique. To illustrate the occurring pitfalls we consider an example in $\mathbf{Z}/30\mathbf{Z}$. It is easy to see that $\overline{a} = \overline{6}$ and $\overline{b} = \overline{10}$ satisfy $(\overline{a}, \overline{b}) = (\overline{g})$ with $g = \overline{2}$. This shows that $\overline{g}$ is a greatest common divisor of $\overline{a}$ and $\overline{b}$. We now want to divide by $\overline{g}$. While the equations $\overline{g} \cdot \overline{18} = \overline{a}$ and $\overline{g} \cdot \overline{20} = \overline{b}$ show that $\overline{18}$ and $\overline{20}$ are valid quotients, they are not coprime in $\mathbf{Z}/30\mathbf{Z}$ as $(\overline{18}, \overline{20}) = (\overline{2})$. This is in total contrast to the situation of integral domains, where dividing by a greatest common divisor produces coprime elements. Here we can try to find coprime quotients by choosing different ones. Now $\overline{g} \cdot \overline{3} = \overline{a}$ and $\overline{g} \cdot 5 = \overline{b}$ show that $\overline{3}$ and $\overline{5}$ will also do and they are fortunately coprime in $\mathbf{Z}/30\mathbf{Z}$.

We now prove that this is always possible by choosing the quotients as small as possible with respect to the Euclidean function.

PROPOSITION 3. *Let $\overline{a}, \overline{b} \in (\mathcal{O}/\mathfrak{m})$. Then the following hold.*

(i) *The element $\overline{b}$ divides $\overline{a}$ if and only if $(a, \mathfrak{m})(b, \mathfrak{m})^{-1}$ is an integral ideal.*
(ii) *An element $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ satisfies $\overline{b}\overline{c} = \overline{a}$ if and only if $(c, \mathfrak{m}) \subseteq (a, \mathfrak{m})(b, \mathfrak{m})^{-1}$.*
(iii) *If $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ satisfies $\overline{b}\overline{c} = \overline{a}$, then $\varphi(\overline{a})/\varphi(\overline{b})$ divides $\varphi(\overline{c})$.*
(iv) *Let $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ such that $\overline{b}\overline{c} = \overline{a}$. Then $\varphi(\overline{a})/\varphi(\overline{b}) = \varphi(\overline{c})$ is equivalent to $(\overline{c}) = \overline{(a, \mathfrak{m})(b, \mathfrak{m})^{-1}}$.*
(v) *Let $\overline{g} \in (\mathcal{O}/\mathfrak{m})$ be a greatest common divisor of $\overline{a}, \overline{b}$, that is, $(\overline{g}) = (\overline{a}, \overline{b})$. Assume that $\overline{e}, \overline{f}$ are elements of $(\mathcal{O}/\mathfrak{m})$ such that $\overline{e}\overline{g} = \overline{a}$, $\overline{f}\overline{g} = \overline{b}$, $\varphi(\overline{e}) = \varphi(\overline{a})/\varphi(\overline{g})$ and $\varphi(\overline{f}) = \varphi(\overline{b})/\varphi(\overline{g})$. Then $\overline{e}$ and $\overline{f}$ are coprime, that is, $(\overline{e}, \overline{f}) = (\mathcal{O}/\mathfrak{m})$.*

Proof. (i) This follows from the fact that $\overline{b} \mid \overline{a}$ is equivalent to $\overline{b}_\mathfrak{p} \mid \overline{a}_\mathfrak{p}$ for all prime divisors $\mathfrak{p}$ of $\mathfrak{m}$.

(ii) For each prime divisor $\mathfrak{p}$ of $\mathfrak{m}$ we have $\overline{b}_\mathfrak{p}\overline{c}_\mathfrak{p} = \overline{a}_\mathfrak{p}$. If $\overline{a}_\mathfrak{p} \neq 0$ (and therefore $\overline{b}_\mathfrak{p} \neq 0$) this is equivalent to $v_\mathfrak{p}(c) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b) = v_\mathfrak{p}((a, \mathfrak{m})(b, \mathfrak{m})^{-1})$. If $\overline{a}_\mathfrak{p} = \overline{b}_\mathfrak{p} = 0$ then this is equivalent to $v_\mathfrak{p}(c) \geqslant 0 = v_\mathfrak{p}((a, \mathfrak{m})(b, \mathfrak{m})^{-1})$. If $\overline{a}_\mathfrak{p} = 0$ and $\overline{b}_\mathfrak{p} \neq 0$, then this is equivalent to $v_\mathfrak{p}(c) \geqslant v_\mathfrak{p}(\mathfrak{m}) - v_\mathfrak{p}(b) = v_\mathfrak{p}((a, \mathfrak{m})(b, \mathfrak{m})^{-1})$. Now the claim follows.

(iii) and (iv) These follow from (ii).

(v) Note that $(g, \mathfrak{m}) = (a, b, \mathfrak{m})$. By (ii) the assumption on the Euclidean function implies $(e, \mathfrak{m}) = (a, \mathfrak{m})(a, b, \mathfrak{m})^{-1}$ and $(f, \mathfrak{m}) = (b, \mathfrak{m})(a, b, \mathfrak{m})^{-1}$. From this one deduces that $(e, f, \mathfrak{m}) = \mathcal{O}$, that is, $(\overline{e}, \overline{f}) = (\mathcal{O}/\mathfrak{m})$. □

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

3. *Basic operations*

In order to describe the complexity of our algorithms we will rely on a modified notion of basic operations introduced by Mulders and Storjohann in [17]. Let (R, φ) be a Euclidean ring and $a, b \in R$. Then a *basic operation* is one of the following.

(B1) For $* \in \{+, -, \cdot\}$ return $a * b$.
(B2) If b divides a in R return an element $\mathsf{div}(a, b) = c \in R$ such that $bc = a$.
(B3) If $b \neq 0$ return $\mathsf{eudiv}(a, b) = (q, r) \in R^2$ such that $a = qb + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$.
(B4) Return $\mathsf{xgcd}(a, b) = (g, s, t, u, v) \in R^5$ such that $(g) = (a, b)$, $g = sa + tb$, $ua + vb = 0$ and $sv - ut = 1$, that is,

$$\begin{pmatrix} g & 0 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} s & u \\ t & v \end{pmatrix}$$

and the transformation matrix is unimodular.
(B5) Return $\mathsf{Ann}(a) = c$ such that $(c) = \mathrm{Ann}(a) = \{r \in R \mid ra = 0\}$.

Note that in [17] it is shown that in the case of $R = \mathbf{Z}/N\mathbf{Z}$ operations (B1) through (B5) can be performed using $O(M(\log(N)\log(\log(N))))$ bit operations, where $M(t)$ is a bound on the number of bit operations required to multiply two $\lceil t \rceil$-bit integers.

We now turn to the case $R = (\mathcal{O}/\mathfrak{m})$, for which there exists an additional basic operation.

(B6) Given an integral ideal $\mathfrak{a}$ of $\mathcal{O}$, return an element $\mathsf{gen}(\mathfrak{a}) = \overline{c} \in (\mathcal{O}/\mathfrak{m})$ such that $\overline{\mathfrak{a}} = (\overline{c})$ in $(\mathcal{O}/\mathfrak{m})$.

We now want to show how each basic operation (Bi) in $(\mathcal{O}/\mathfrak{m})$, $1 \leqslant i \leqslant 6$, can be solved algorithmically using basic operations in $\mathbf{Z}/N\mathbf{Z}$, where $N = \mathbf{N}(\mathfrak{m})$ is the norm of $\mathfrak{m}$. We assume that we are given $\mathbf{Z}$-bases $(\omega_i)_{1 \leqslant i \leqslant d}$ and $(\nu_i)_{1 \leqslant i \leqslant d}$ of $\mathcal{O}$ and $\mathfrak{m}$ respectively such that $\nu_i = n_i \omega_i$ with integers $n_i \in \mathbf{Z}_{\geqslant 1}$, $1 \leqslant i \leqslant d$, that is, the basis matrix of $\mathfrak{m}$ is diagonal. Then the map

$$(\mathcal{O}/\mathfrak{m}) \longrightarrow (\mathbf{Z}/n_1\mathbf{Z}) \times \ldots \times (\mathbf{Z}/n_d\mathbf{Z}), \quad \overline{\sum_i a_i \omega_i} \longmapsto (\overline{a}_1, \ldots, \overline{a}_d)$$

is an isomorphism of abelian groups which we use to identify $(\mathcal{O}/\mathfrak{m})$ with $\prod_i \mathbf{Z}/n_i\mathbf{Z}$.

Evaluating the canonical map $\mathcal{O} \to (\mathcal{O}/\mathfrak{m})$ at an element $\sum_i a_i \omega_i$ consists of d divisions with remainder and the addition of two elements in $(\mathcal{O}/\mathfrak{m})$ consists of d additions in $\mathbf{Z}/n_i\mathbf{Z}$. As the above map is not multiplicative, multiplication of two elements $\overline{a} = (\overline{a}_1, \ldots, \overline{a}_d)$, $\overline{b} = (\overline{b}_1, \ldots, \overline{b}_d) \in (\mathcal{O}/\mathfrak{m})$ is more involved. More precisely the element $\overline{c} = (\overline{c}_1, \ldots, \overline{c}_d) \in (\mathcal{O}/\mathfrak{m})$ with $\overline{a}\overline{b} = \overline{c}$ is given by

$$\overline{c}_k = \overline{\sum_i \sum_j a_i b_j \Gamma_{i,j}^k} \in (\mathbf{Z}/n_k\mathbf{Z}),$$

where $(\Gamma_{i,j}^k)_{i,j,k}$ denotes the structure constants of the $\mathbf{Z}$-algebra $\mathcal{O}$ with respect to the basis $(\omega_i)_{1 \leqslant i \leqslant d}$. Thus for each $1 \leqslant k \leqslant d$ we need d^2 basic operations in $(\mathbf{Z}/n_k\mathbf{Z})$ to compute $\overline{c}_k$.

To accomplish (B2), denote by $M_b \in \mathbf{Z}^{d \times d}$ the representation matrix of $\mathcal{O} \to \mathcal{O}, x \mapsto bx$ with respect to (ω_i), where each entry is reduced modulo N, and by $M_{\mathfrak{m}}$ the diagonal basis matrix of $\mathfrak{m}$. Then $\overline{a} = \overline{b}\overline{c}$ for some element $c \in (\mathcal{O}/\mathfrak{m})$ if and only if the equation $(M_b | M_{\mathfrak{m}})X = a$ is solvable. As this linear system can be solved modulo N, we need $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$. Note that the kernel of this matrix is (the lift) of $\mathrm{Ann}(\overline{b})$, the annihilator of $\overline{b}$ in $(\mathcal{O}/\mathfrak{m})$.

So far we have shown that operations (B1) and (B2) can be performed using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$ (for the sake of simplicity a basic operation in $\mathbf{Z}/k\mathbf{Z}$ with $1 \leqslant k \leqslant N$ is counted as a basic operation in $\mathbf{Z}/N\mathbf{Z}$).

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

We now turn to the more involved operations (Bi), $3 \leqslant i \leqslant 6$, the big difference to (B1) being the non-uniqueness of the operations (again mainly due to the presence of zero-divisors). Using the Chinese remainder theorem we will see that the defining properties of the operations can be stated purely in terms of valuations at each prime ideal dividing $\mathfrak{m}$. Therefore the main task will be the construction of integral elements with prescribed behavior at a finite set of prime ideals. While there exist deterministic algorithms for these kinds of problems, they have the major flaw that they need a costly prime ideal factorization of $\mathfrak{m}$. To overcome this difficulty, in this article we will pursue the idea of probabilistic algorithms. More precisely our algorithms will be of Las Vegas type with expected polynomial running time, which can be easily turned into Monte Carlo algorithms if wished. The running time of our algorithms will depend on the value

$$p_{\mathfrak{m}} = \frac{|(\mathcal{O}/\mathfrak{m})^\times|}{|(\mathcal{O}/\mathfrak{m})|} = \prod_{\mathfrak{p}\mid\mathfrak{m}} \left(1 - \frac{1}{\mathbf{N}(\mathfrak{p})}\right).$$

In § 5 we will discuss the size of $p_{\mathfrak{m}}$ and the applicability of the presented algorithms.

We assume that we have access to an oracle producing random elements in any finite ring of the form $\mathbf{Z}/k\mathbf{Z}$, $k \in \mathbf{Z}_{>0}$. During the complexity analysis we will omit the costs of calling this oracle.

3.1. *Euclidean function and division with remainder*

LEMMA 4. *Let $\overline{a} \in (\mathcal{O}/\mathfrak{m})$. Computing $\varphi(\overline{a})$ can be done using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.*

Proof. We first compute the d products $\overline{a\omega_i}$ for $1 \leqslant i \leqslant d$ using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$. Denoting by $\gamma_1, \ldots, \gamma_d$ the canonical lifts of these elements we know that $\gamma_1, \ldots, \gamma_d, \nu_1, \ldots, \nu_d$ constitute a $\mathbf{Z}$-generating system of $(a) + \mathfrak{m}$. Computing the Hermite normal form basis of this generating system can then be done using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$ while the norm computation takes $O(d)$ such operations. □

ALGORITHM 1 (Probabilistic Euclidean division). *Let $\overline{a}, \overline{b} \in (\mathcal{O}/\mathfrak{m})$, $\overline{b} \neq \overline{0}$. The following steps return* $\mathsf{eucdiv}(\overline{a}, \overline{b})$.

(i) *Choose $\overline{q} \in (\mathcal{O}/\mathfrak{m})$ uniformly distributed and compute $\overline{r} = \overline{a} - \overline{q}\overline{b}$.*
(ii) *If $\varphi(\overline{r}) \geqslant \varphi(\overline{a})$ go to Step* (i).
(iii) *Return $(\overline{q}, \overline{r})$.*

LEMMA 5. *Let $\overline{a}, \overline{b} \in (\mathcal{O}/\mathfrak{m})$ such that $\overline{b}$ does not divide $\overline{a}$. For each prime divisor $\mathfrak{p}$ of $\mathfrak{m}$ define*

$$S_{\mathfrak{p}} = \begin{cases} (\mathcal{O}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}), & \text{if } 0 < v_{\mathfrak{p}}(a) < v_{\mathfrak{p}}(b), \\ (\mathcal{O}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})^\times, & \text{if } v_{\mathfrak{p}}(b) < v_{\mathfrak{p}}(a), \\ \{\overline{x} \in (\mathcal{O}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})} \mid \mathbf{N}((a+xb), \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}) \leqslant \mathbf{N}(b, \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})\}, & \text{if } v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(b). \end{cases}$$

Then the following hold.

(i) *If $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ is an element such that $\overline{c}_{\mathfrak{p}} \in S_{\mathfrak{p}}$ for all prime divisors $\mathfrak{p}$ of $\mathfrak{m}$, then $\varphi(\overline{a}+\overline{b}\overline{c}) < \varphi(\overline{b})$.*
(ii) *We have $\{\overline{c} \in (\mathcal{O}/\mathfrak{m}) \mid \varphi(\overline{a} + \overline{b}\overline{c}) < \varphi(\overline{b})\} \geqslant |(\mathcal{O}/\mathfrak{m})^\times|$.*
(iii) *If $\overline{q} \in (\mathcal{O}/\mathfrak{m})$ is uniformly distributed in $(\mathcal{O}/\mathfrak{m})$, then the probability that $\overline{a} = \overline{q}\overline{b}+(\overline{a}-\overline{q}\overline{b})$ is a Euclidean division is at least $p_{\mathfrak{m}}$.*

Proof. (i) Let $\overline{c}_{\mathfrak{p}} \in S_{\mathfrak{p}}$. In the second and third case we have $v_{\mathfrak{p}}(a + bc) \leqslant v_{\mathfrak{p}}(b)$ while in the first case we have $v_{\mathfrak{p}}(a + bc) = v_{\mathfrak{p}}(a) < v_{\mathfrak{p}}(b)$. Since $\overline{b}$ does not divide $\overline{a}$ there exists a prime

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

divisor $\mathfrak{p}$ of $\mathfrak{m}$ such that $0 < v_\mathfrak{p}(a) < v_\mathfrak{p}(b)$ implying that $\mathbf{N}((a+bc), \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}) < \mathbf{N}(b, \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})$. Thus we have $\varphi(\overline{a} + \overline{b}\overline{c}) < \varphi(\overline{b})$.

(ii) It remains to show $|S_\mathfrak{p}| \geqslant |(\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})^\times|$ in the case $v_\mathfrak{p}(a) = v_\mathfrak{p}(b)$. If $v_\mathfrak{p}(b) \geqslant v_\mathfrak{p}(\mathfrak{m})$, then $S_\mathfrak{p} = \mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}$ and we are done. Therefore let $v_\mathfrak{p}(b) < v_\mathfrak{p}(\mathfrak{m})$ and consider the natural map $\pi\colon (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}) \to (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(b)+1})$. The set $\pi(S_\mathfrak{p})$ is the complement of the set of solutions $\overline{a} = -\overline{b}\overline{x}$ with $\overline{x} \in (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(b)+1})$. As this equation has $\mathbf{N}((b), \mathfrak{p}^{v_\mathfrak{p}(b)+1}) = \mathbf{N}(\mathfrak{p}^{v_\mathfrak{p}(b)})$ solutions we have $|\pi(S_\mathfrak{p})| = \mathbf{N}(\mathfrak{p}^{v_\mathfrak{p}(b)+1}) - \mathbf{N}(\mathfrak{p}^{v_\mathfrak{p}(b)})$. It follows that $|S_\mathfrak{p}| = \mathbf{N}(\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{m})-(v_\mathfrak{p}(b)+1)}|\pi(S_\mathfrak{p})| = |(\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})^\times|$.

(iii) This follows from (ii). □

PROPOSITION 6. *Algorithm 1 is correct and the expected number of basic operations in* $\mathbf{Z}/N\mathbf{Z}$ *is* $O((1/p_\mathfrak{m})d^3)$.

Proof. We need to count the expected number of repetitions of Step (i). It is easy to see that for $i \in \mathbf{Z}_{\geqslant 1}$, with probability $p_\mathfrak{m}(1-p_\mathfrak{m})^{i-1}$ the number of repetitions of Step (i) is i. Thus the expected number is $p_\mathfrak{m}\sum_{i=1}^{\infty} i(1-p_\mathfrak{m})^{i-1} = p_\mathfrak{m}(1/p_\mathfrak{m} + (1-p_\mathfrak{m})/p_\mathfrak{m}^2) = 1/p_\mathfrak{m}$. Now the claim follows as Step (i) needs $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$. □

3.2. *Finding a generator of an ideal and computing the annihilator*

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. It is easy to see that for an element $c \in \mathcal{O}$ the equation $(\overline{c}) = \overline{\mathfrak{a}}$ holds if and only if for all prime divisors $\mathfrak{p}$ of $\mathfrak{m}$ we have $v_\mathfrak{p}(c) = v_\mathfrak{p}(\mathfrak{a}, \mathfrak{m})$.

ALGORITHM 2. *Let* $\mathfrak{a}$ *be an integral of* $\mathcal{O}$. *The following steps return* $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ *such that* $(\overline{c}) = \overline{\mathfrak{a}}$.

(i) *Compute* $(\mathfrak{a}, \mathfrak{m})$.
(ii) *Choose* $\overline{c} \in (\mathfrak{a}, \mathfrak{m})/(N^2)$ *uniformly distributed.*
(iii) *If* $(\mathfrak{a}, \mathfrak{m}) \neq (N, c)$ *go to Step* (ii).
(iv) *Return* $\overline{c} \in (\mathcal{O}/\mathfrak{m})$.

LEMMA 7. *Algorithm 2 is correct and the expected number of basic operations in* $\mathbf{Z}/N\mathbf{Z}$ *is* $O((1/p_\mathfrak{m})d^3)$.

Proof. We prove the following: if $\mathfrak{a}$ is an integral ideal of $\mathcal{O}$ and $\overline{c}$ is chosen uniformly in $(\mathfrak{a}, \mathfrak{m})/(N^2)$, then the probability that $(\mathfrak{a}, \mathfrak{m}) = (N, c)$ is $p_\mathfrak{m}$. Let $\mathfrak{b} = (\mathfrak{a}, \mathfrak{m})$ and fix one prime divisor $\mathfrak{p}$ of $\mathfrak{m}$. We want to count the elements $\overline{c} \in \mathfrak{b}/(N^2)$ such that $v_\mathfrak{p}(c) = v_\mathfrak{p}(\mathfrak{b})$. Note that $v_\mathfrak{p}(N^2) > v_\mathfrak{p}(\mathfrak{b})$ and therefore $c \in \mathfrak{b} \setminus \mathfrak{b}\mathfrak{p}$ is equivalent to $\overline{c} \in \mathfrak{b}/(N^2) \setminus \mathfrak{b}\mathfrak{p}/(N^2)$. Counting the elements in these sets we see that the probability that an element $\overline{c} \in \mathfrak{b}/(N^2)$ satisfies $v_\mathfrak{p}(c) = v_\mathfrak{p}(\mathfrak{a})$ is $(1 - 1/\mathbf{N}(\mathfrak{p}))$.

Note that Step (i) needs $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$. We have already shown that the expected number of executions of Step (iii) is $1/p_\mathfrak{m}$. As each execution consists of $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$, the claim follows. □

LEMMA 8. *Let* $\overline{b} \in (\mathcal{O}/\mathfrak{m})$. *Then we can compute* $\overline{c} = \mathsf{Ann}(\overline{b})$ *with an expected number of* $O((1/p_\mathfrak{m})d^3)$ *basic operations in* $\mathbf{Z}/N\mathbf{Z}$.

Proof. After computing the annihilator as the kernel of M_b modulo N (as for (B2)) using $O(d^3)$ basic operations, we apply Algorithm 2 to obtain a generator. □

3.3. *Extended GCD computation*

We now turn to the xgcd problem. In the case of the rational integers $\mathbf{Z}$ the task is easy: if g is a greatest common divisor of two integers $a, b \in \mathbf{Z}$ we can compute $s, t \in \mathbf{Z}$ such that

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

$g = sa + tb$. Then

$$\begin{pmatrix} g & 0 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} s & -t/g \\ t & s/g \end{pmatrix}$$

and we are done. While we can of course just use the normal Euclidean algorithm to find the cofactors, this is, in our case, rather expensive as each Euclidean division requires a random search. On the other hand, computing the GCD directly using ideals takes only *one* random search.

As the underlying idea is that dividing by a greatest common divisor produces coprime elements, the example at the end of § 2 shows that we cannot blindly adapt this in the presence of zero-divisors. Fortunately Proposition 3 shows that there exist minimal quotients $\overline{e}, \overline{f}$ with respect to the Euclidean function such that $\overline{e}\overline{g} = \overline{a}$, $\overline{f}\overline{g} = \overline{b}$ and $(\overline{e}, \overline{f}) = (\mathcal{O}/\mathfrak{m})$. In particular there exist $\overline{u}, \overline{v} \in (\mathcal{O}/\mathfrak{m})$ such that $\overline{e}\overline{u} + \overline{f}\overline{v} = 1$. A quick calculation shows that

$$\begin{pmatrix} \overline{g} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \end{pmatrix} \begin{pmatrix} \overline{u} & -\overline{f} \\ \overline{v} & \overline{e} \end{pmatrix}$$

is a unimodular transformation implying that $\mathsf{xgcd}(\overline{a}, \overline{b}) = (\overline{g}, \overline{u}, \overline{v}, -\overline{f}, \overline{e})$ is valid.

In order to apply this we need to explain how to find minimal quotients and how to express a greatest common divisor as a linear combination.

LEMMA 9.

(i) *Let $\overline{b}$ be a divisor of $\overline{a}$. An element $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ with $\overline{c}\overline{b} = \overline{a}$ and $\varphi(\overline{c}) = \varphi(\overline{a})/\varphi(\overline{b})$ can be computed using an expected number of $O((1/p_{\mathfrak{m}})d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.*

(ii) *Let $\overline{e}, \overline{f} \in (\mathcal{O}/\mathfrak{m})$ be such that $(\overline{e}, \overline{f}) = (\mathcal{O}/\mathfrak{m})$. Then $\overline{u}, \overline{v}$ with $\overline{u}\overline{e} + \overline{v}\overline{f} = 1$ can be computed using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.*

(iii) *Let $\overline{a}, \overline{b} \in (\mathcal{O}/\mathfrak{m})$. Then $\mathsf{xgcd}(\overline{a}, \overline{b})$ can be computed with an expected number of $O((1/p_{\mathfrak{m}})d^3)$ basic operations.*

Proof. (i) Using (B2) we can compute a fixed quotient $\overline{c}_0$. Moreover we have seen that at the same time we obtain a basis of an ideal $\mathfrak{a}$ of $\mathcal{O}$ with $\overline{\mathfrak{a}} = \mathrm{Ann}(\overline{b})$. Invoking (B6) we can compute a generator of the ideal $\overline{\mathfrak{a}}$. Now we choose uniformly distributed elements $\overline{q} \in \overline{\mathfrak{a}}$ until $\varphi(\overline{c}_0 + \overline{q}) = \varphi(\overline{a})/\varphi(\overline{b})$. If this is the case then $\overline{c}_0 + \overline{q}$ is a quotient which is minimal with respect to the Euclidean function. Proposition 3 shows that if $\overline{q}$ is uniformly distributed in $\mathrm{Ann}(\overline{b})$, then $\overline{c}_0 + \overline{q}$ is uniformly distributed in $\overline{(a, \mathfrak{m})(b, \mathfrak{m})^{-1}}$. Now the claim follows from Lemma 1.

(ii) As in the case of division, we see that the set of tuples $(\overline{x}, \overline{y}) \in (\mathcal{O}/\mathfrak{m})^2$ with $\overline{x}\overline{e} + \overline{y}\overline{f} = \overline{1}$ is the set of solutions of a $d \times 3d$ matrix with entries in $\mathbf{Z}$. As in addition this system can be solved modulo N, the task of finding a suitable tuple $(\overline{x}, \overline{y})$ can be solved using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.

(iii) Follows from (ii) and (iii). □

COROLLARY 10. *Any basic operation in $(\mathcal{O}/\mathfrak{m})$ can be performed with an expected number of $O((1/p_{\mathfrak{m}})d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.*

4. *Applications to matrix normal forms*

When working with algebraic number fields the objects of desire often carry the structure of finitely generated torsion-free modules over $\mathbf{Z}$. While the structure theorem for modules over $\mathbf{Z}$ asserts the freeness of such modules, the Hermite normal form (HNF) and algorithms for computing it bring them fully under control. They not only allow for the computation of a basis given a generating set, but they also enable us to solve various algorithmic problems.

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

Based on the extended GCD, it is straightforward to formulate a naive algorithm for computing the HNF over $\mathbf{Z}$. Unfortunately, as in the case of Gaußian elimination over $\mathbf{Q}$, coefficient swell occurs. Although there are various techniques to handle this circumstance, the most natural one is the use of residual methods, which goes back to Iliopoulos [13] and Domich, Kannan and Trotter [9]: instead of computing the HNF over $\mathbf{Z}$, one computes a normal form over $\mathbf{Z}/d\mathbf{Z}$ for some $d \in \mathbf{Z}$ and lifts the result back to $\mathbf{Z}$. If d is chosen to be a multiple of the determinant of the lattice spanned by the rows of the matrix, this will yield a correct result.

The aim of this section is to introduce residual methods to the computation of normal forms of $\mathcal{O}$-modules by passing to a quotient ring $(\mathcal{O}/\mathfrak{m})$ for some suitable integral ideal $\mathfrak{m}$ and by lifting the result back to $\mathcal{O}$.

4.1. *Strong echelon form for principal ideal rings*

Given a ring R and a matrix $A \in R^{n\times m}$ denote by $S(A) \subseteq R^m$ the row span of A. The idea of attaching a unique matrix normal form to submodules of R^m, where R is a principal ideal ring, goes back to Howell [12]. He introduced a normal form (now called the *Howell normal form*) of submodules of $(\mathbf{Z}/d\mathbf{Z})^m$ and an algorithm for computing it, such that two modules are equal if and only if their Howell normal forms coincide. In his PhD thesis Storjohann [16] has generalized this notion to arbitrary principal ideal rings.

In this article we will adapt the Howell normal form to our needs. For an R-module $M \subseteq R^m$ and $1 \leqslant i \leqslant m$ we define $S_i(M)$ to be the set of all elements of M with last i entries zero. For convenience we set $S_i(A) = S_i(S(A))$ if A is matrix over R with m columns.

Definition 11. Let $M \subseteq R^m$ be an R-module. A matrix $H = (h_{ij}) \in R^{n\times m}$, $n \geqslant m$, is called a *strong echelon form* of M if and only if:

(S1) for $1 \leqslant i \leqslant m$ the ith row of H is zero or $i = \max\{1 \leqslant j \leqslant m \mid h_{ij} \neq 0\}$. For $i > m$ the ith row of H is zero;

(S2) for $1 \leqslant i \leqslant m$ the rows $1, \ldots, i$ generate $S_{m-i}(M)$.

To illustrate the definitions consider the following matrices over $\mathbf{Z}/6\mathbf{Z}$:

$$A = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{1} & \overline{3} \end{pmatrix}, \quad B = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{5} & \overline{3} \end{pmatrix}, \quad C = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{2} & \overline{0} \\ \overline{5} & \overline{3} \end{pmatrix}, \quad D = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{5} & \overline{3} \\ \overline{0} & \overline{0} \end{pmatrix}.$$

It is easy to see that they have the same span. While the matrix A has a minimal number of non-zero rows the element $(\overline{2}, \overline{0}) \in S(A)$ shows that A does not satisfy (S2). On the other hand the matrix C violates (S1). Thus only B and D are strong echelon forms of M.

A few words on the relation between the strong echelon form and the Howell normal form: in contrast to the Howell normal form we 'order' the basis elements. This will be important in § 4.2 where we describe the combination of strong echelon forms. Note that we will use the strong echelon form over $(\mathcal{O}/\mathfrak{m})$ only as an auxiliary step to obtain normal forms over $\mathcal{O}$. Since this does not require the strong echelon form to be unique, this explains the absence of appropriate restrictions in the definition. For working with $(\mathcal{O}/\mathfrak{m})$-modules themselves we can recover uniqueness easily by the following steps. We have to show how to find a fixed representative modulo $(\mathcal{O}/\mathfrak{m})^\times$ and modulo $(\overline{d})$ for some $\overline{d} \in (\mathcal{O}/\mathfrak{m})$. The former problem can be solved by noting that if $\overline{a}$ is an element of $(\mathcal{O}/\mathfrak{m})$, then the coset of $\overline{a}$ modulo $(\mathcal{O}/\mathfrak{m})^\times$ is equal to the set of all $\overline{b} \in (\mathcal{O}/\mathfrak{m})$ with $(b, \mathfrak{m}) = (a, \mathfrak{m})$. Thus by choosing a generator of $\overline{(a, \mathfrak{m})}$ in a deterministic way we obtain a unique representative. By reducing the off-diagonal elements modulo the unique HNF basis of $(d, \mathfrak{m})$, where d is the corresponding diagonal entry, we obtain unique representatives for the off-diagonal elements.

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

Based on Howell's approach Storjohann and Mulders describe in [17] a simple algorithm for computing the Howell normal form over $\mathbf{Z}/d\mathbf{Z}$, which easily generalizes to any ring supporting basic operations (Bi), $1 \leqslant i \leqslant 6$. The following modified version yields a strong echelon form.

ALGORITHM 3 (Strong echelon form over principal ideal rings). *Let $A \in R^{n\times m}$ be a matrix with $n \geqslant m$. The following steps return a strong echelon form of A.*

(i) (*This puts A into triangular form.*) *For $1 \leqslant i < j \leqslant n$ compute $(g, s, t, u, v) = \mathsf{xgcd}(a_{j,i}, a_{j,j})$ and set*

$$\begin{pmatrix} A_j \\ A_i \end{pmatrix} = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} A_j \\ A_i \end{pmatrix}.$$

(ii) *Augment A with one zero row.*

(iii) *For $1 \leqslant j \leqslant m$ do the following.*

  (a) *If $a_{j,j} \neq 0$ compute $c = \mathsf{Ann}(a_{j,j})$ and set $A_{n+1} = cA_j$. If $a_{j,j} = 0$ then set $A_{n+1} = A_j$.*

  (b) *For $j + 1 \leqslant i \leqslant m$ compute $(g, s, t, u, v) = \mathsf{xgcd}(a_{i,i}, a_{n+1,i})$ and set*

$$\begin{pmatrix} A_i \\ A_{n+1} \end{pmatrix} = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} A_i \\ A_{n+1} \end{pmatrix}.$$

(iv) *Sort the rows such that (S1) is satisfied.*

(v) *Return A.*

4.2. *Modular computation of a strong echelon form*

One of the reasons we have introduced the strong echelon form (instead of using the equally unknown Howell normal form) is the important fact that it allows for efficient residual computations. To be more precise let R be a principal ideal ring and $a, b, e, f \in R$ elements such that $ab = 0$ and $1 = ea + fb$. Denote by π_a and π_b the canonical projections of R onto $R/(a)$ and $R/(b)$ respectively. By abuse of notation we also denote the induced projections $R^m \to (R/(a))^m$ and $R^{n\times m} \to (R/(a))^{n\times m}$ by π_a; we do the same for π_b. Then for any R-module $M \subseteq R^m$ the equation

$$M = 1M = eaM + fbM = ea(M + bR^m) + fb(M + aR^m) \tag{4.1}$$

holds. As $M + aR^m = \pi_a^{-1}(\pi_a(M))$ and $M + bR^m = \pi_b^{-1}(\pi_b(M))$ we see that M can be obtained by lifting the modules $\pi_a(M)$ and $\pi_b(M)$, which are now living over the (hopefully 'smaller') rings $R/(a)$ and $R/(b)$, back to R. The following lemma shows that by using the strong echelon form the lifting procedure comes for free.

LEMMA 12. *Assume that $A \in R^{n\times m}$ is a matrix such that $\pi_a(A) \in (R/(a))^{n\times m}$ is a strong echelon form of $\pi_a(M)$ and every non-zero diagonal element of A is a divisor of a. Then A is a strong echelon form of $M + aR^m$.*

Proof. Given $v \in S_j(M + aR^m)$ we want to show that $v \in S(A)$. We prove the statement by induction on j. If $\pi_a(v_j) = 0$, then v_j is a multiple of a. In particular there exists $r \in R$ such that $v - rA_j \in S_{j+1}(M + aR^m)$. If $\pi_a(v_j) \neq 0$ then property (S1) implies that there exists $r_i \in R$ with $v - \sum_{i=1}^{j} r_i A_i \in S_j(aR^m)$. Thus again there exists $r \in R$ such that $v = \sum_{i=1}^{j} r_i A_i - rA_j \in S_{j+1}(M + aR^m)$. This implies $M + aR^m = S(A)$ and at the same time we have shown that A satisfies properties (S1) and (S2). □

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

Thus by computing strong echelon forms over $R/(a)$ and $R/(b)$ we can compute strong echelon forms of $M + aR^m$ and $M + bR^m$. We now turn to the recombination step. Let A and B be strong echelon forms of $M + aR^m$ and $M + bR^m$ respectively. By padding A or B with zero rows we may assume that A and B have the same number of rows.

LEMMA 13. *The matrix $fbA + eaB$ is a strong echelon form of M.*

Proof. Firstly we show $M = S(fbA + eaB)$. Equation (4.1) implies that M is generated by fbA_i, eaB_i, $1 \leqslant i \leqslant n$. Therefore it is sufficient to prove $fbA_i, eaB_i \in S(fbA + eaB)$. As fb is an idempotent, that is, $(fb)^2 = fb$, we have $fbA_i = (fb)^2A_i + (fb)(ea)B_i = fb(fbA_i + eaB_i) \in S(fbA + eaB)$ and analogously $eaB_i \in S(fbA + eaB)$.

Sine eaB and fbA have property (S1), so does the sum. Property (S2) follows by decomposing an element $v \in M$ into $v = fbv + eav$ and applying property (S2) of eaB and fbA. □

Now let $\mathfrak{m}$ and $\mathfrak{n}$ be coprime integral ideals of $\mathcal{O}$. We want to apply the preceding discussion to the computation of a strong echelon form of an $(\mathcal{O}/\mathfrak{mn})$-module M. Denote by $\overline{a}$ and $\overline{b}$ generators of the ideals $\overline{\mathfrak{m}}$ and $\overline{\mathfrak{n}}$ in $(\mathcal{O}/\mathfrak{mn})$. Then $\overline{a}\overline{b} = 0$, and $(\mathcal{O}/\mathfrak{mn})/(\overline{a})$ and $(\mathcal{O}/\mathfrak{mn})/(\overline{b})$ are isomorphic to $\mathcal{O}/\mathfrak{m}$ and $\mathcal{O}/\mathfrak{n}$ respectively. We have canonical projections $\pi_a = \pi_{\mathfrak{m}} \colon (\mathcal{O}/\mathfrak{mn}) \to (\mathcal{O}/\mathfrak{m})$ and $\pi_b = \pi_{\mathfrak{n}} \colon (\mathcal{O}/\mathfrak{mn}) \to (\mathcal{O}/\mathfrak{n})$. As $\overline{a}$ and $\overline{b}$ are coprime, we can compute $\overline{e}, \overline{f} \in (\mathcal{O}/\mathfrak{mn})$ such that $\overline{e}\overline{a} + \overline{f}\overline{b} = 1$. Thus we are in a situation where we can apply Lemmas 12 and 13. The only missing step is the normalization of the diagonal elements in the assumption of Lemma 13.

We assume that A' is a matrix over $(\mathcal{O}/\mathfrak{mn})$ such that $\pi_{\mathfrak{m}}(A')$ is a strong echelon form of $\pi_{\mathfrak{m}}(M)$. We define a new matrix A over $(\mathcal{O}/\mathfrak{mn})$ by setting the ith row A_i to be

$$A_i = \overline{b}A'_i + (\overline{a}\delta_{i,j})_{1 \leqslant j \leqslant n}$$

for $1 \leqslant i \leqslant n$, where $\delta_{i,j}$ denotes the Kronecker delta. As $\overline{b}$ is a unit modulo $\mathfrak{m}$ and $\pi_{\mathfrak{m}}(\overline{a}) = 0$, the matrix $\pi_{\mathfrak{m}}(A)$ is also a strong echelon form of $\pi_{\mathfrak{m}}(M)$. We claim that A satisfies the assumption of Lemma 12. To prove this we show that for all $\overline{d} \in (\mathcal{O}/\mathfrak{mn})$ the element $\overline{b}\overline{d} + \overline{a}$ is a divisor of $\overline{a}$ in $(\mathcal{O}/\mathfrak{mn})$. Note that this is equivalent to $\min(v_{\mathfrak{p}}(bd + a), v_{\mathfrak{p}}(\mathfrak{mn})) \leqslant \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(\mathfrak{mn}))$ for all prime divisors $\mathfrak{p}$ of $\mathfrak{mn}$. If $\overline{d} = 0$ this holds obviously. Therefore we may assume $\overline{d} \neq 0$. But then the claim follows easily by noting that $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(\mathfrak{m})$ if $\mathfrak{p} \mid \mathfrak{m}$ and $v_{\mathfrak{p}}(b) > 0 = v_{\mathfrak{p}}(a)$ if $\mathfrak{p} \mid \mathfrak{n}$.

4.3. *Normal forms for modules over $\mathcal{O}$*

Since $\mathcal{O}$ is in general not a principal ideal domain, finitely generated torsion-free modules over $\mathcal{O}$ are not necessarily free. For this reason the connection between such modules and matrix normal forms is more subtle than in the principal ideal domain case. While for any $\mathcal{O}$-module $M \subseteq \mathcal{O}^m$ there exists some matrix $A \in \mathcal{O}^{m \times n}$ such that $S(A) = M$, we cannot expect to find a triangular shaped matrix with this property. For if this is the case, M is the direct sum of the rows of A and therefore free over $\mathcal{O}$.

Although $\mathcal{O}$ is not a principal ideal domain, the properties of being a Dedekind ring are strong enough to prove a weakened classification theorem of $\mathcal{O}$-modules. More precisely Steinitz [**14**, **15**] has shown that there exists fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ of K and a matrix $A \in K^{n \times m}$ with rows $A_1, \ldots, A_n$ such that $M = \mathfrak{a}_1A_1 \oplus \ldots \oplus \mathfrak{a}_nA_n$. To work with these objects, Cohen [**7**] has introduced the notion of a *pseudomatrix*, which is just a pair $((\mathfrak{a}_i)_{1 \leqslant i \leqslant n}, A)$ consisting of a family of fractional ideals of K (the *coefficient ideals*) and a matrix $A \in K^{n \times m}$. If $\mathcal{P} = ((\mathfrak{a}_i)_i, A)$ is such a pseudomatrix, we define $S(\mathcal{P})$ to be $\sum_{i=1}^{n} \mathfrak{a}_iA_i$, the *span* of the

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

pseudomatrix $\mathcal{P}$. In case $\sum \mathfrak{a}_i A_i = \bigoplus \mathfrak{a}_i A_i$ we call $\mathcal{P}$ a *nice* pseudomatrix. Note that $\mathcal{P}$ is nice if A is of triangular shape.

The problem of computing a nice pseudomatrix goes back to Bosma and Pohst [6]. Based on similar ideas, Cohen introduced in [7] the notion of pseudo Hermite normal form (pseudo-HNF) of a module, similar to the HNF over principal ideal domains, and described an algorithm for computing it. To be more precise, a pseudomatrix $\mathcal{P} = ((\mathfrak{a}_i), A)$ with span M is called *a pseudo-HNF of* M, if A is a lower triangular matrix with 1 being the last non-zero element in each non-zero row. By choosing the off-diagonal elements in fixed sets of coset representatives, the pseudo-HNF of an $\mathcal{O}$-module is unique. Recently, Biasse and Fieker [3] have modified Cohen's algorithm to formulate a provable polynomial time algorithm for computing the pseudo-HNF.

4.4. *From $\mathcal{O}$ to $(\mathcal{O}/\mathfrak{m})$ to $\mathcal{O}$*

Let $\mathcal{P} = ((\mathfrak{a}_i), A)$ be a pseudomatrix. So far the underlying idea of all known algorithms for computing a nice pseudomatrix of $S(\mathcal{P})$ is to transform A into triangular shape, while carefully adjusting the coefficient ideals ensuring that the span does not change. The necessary modifications of the coefficient ideals are the heart and at the same time the bottleneck of these algorithms. In [3] even costly lattice reduction algorithms are necessary to bound the size of the objects during the algorithm and to ensure polynomial time complexity.

We now describe how most of the ideal arithmetic can be avoided by passing to a suitable quotient ring of $\mathcal{O}$. From now on we assume that the span $M = S(\mathcal{P})$ is an $\mathcal{O}$-module of rank m contained in $\mathcal{O}^m$ and $A \in K^{n\times m}$ with $n \geqslant m$. As in the integer case the key idea is that there exists an integral ideal $\mathfrak{m}$ of $\mathcal{O}$ such that $\mathfrak{m}\mathcal{O}^m \subseteq M$. Denote by $\pi_\mathfrak{m}$ the canonical projection $\mathcal{O} \to \mathcal{O}/\mathfrak{m}$ and the induced projections on $\mathcal{O}^m$ and $\mathcal{O}^{n\times m}$.

ALGORITHM 4. *The following steps return a matrix $\overline{B} \in (\mathcal{O}/\mathfrak{m})^{n\times m}$ such that $S(\overline{B}) = \pi_\mathfrak{m}(S(\mathcal{P}))$.*

(i) *For $1 \leqslant i \leqslant n$ find elements $a_i \in K$ such that $\mathfrak{b}_i = a_i\mathfrak{a}_i$ is integral and coprime to $\mathfrak{m}$, and divide row A_i by a_i.*
(ii) *For $1 \leqslant i, j \leqslant m$ write $A_{ij} = a_{ij}/b_{ij}$ with $a_{ij}, b_{ij} \in \mathcal{O}$.*
(iii) *Return $\overline{B} = (\overline{a}_{ij}\overline{b}_{ij}^{-1})_{i,j}$.*

A few remarks on the correctness. Step (i) does not change the span and the new coefficient ideals $\mathfrak{b}_i$, being coprime to $\mathfrak{m}$, satisfy $\pi_\mathfrak{m}(\mathfrak{b}_i) = (\mathcal{O}/\mathfrak{m})$. Moreover the relation $\mathfrak{m}\mathcal{O}^m \subseteq M \subseteq \mathcal{O}^m$ implies that the denominators of all matrix entries are coprime to $\mathfrak{m}$ and thus invertible modulo $\mathfrak{m}$. Finding the elements a_i in Step (i) is just another application of the approximation theorem (see [8, Corollary 1.3.9]) and can therefore be performed using Belabas' algorithm.

Applying Algorithm 3 to the matrix $\overline{B}$ obtained in the preceding algorithm we arrive, after removing zero rows, at a matrix $C \in \mathcal{O}^{m\times m}$ such that $\pi_\mathfrak{m}(C)$ is a strong echelon form of $\pi_\mathfrak{m}(M)$. The connection to the original module M is given by the following lemma.

LEMMA 14. *Assume that $C \in \mathcal{O}^{m\times m}$ is a matrix such that $\pi_\mathfrak{m}(C)$ is a strong echelon form of $\pi_\mathfrak{m}(M)$. Then the pseudomatrix $\mathcal{P}' = (I, C)$ with $I = (\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{m}, \ldots, \mathfrak{m})$ and $D = (C^t|\mathbf{I}_m^t)^t$ satisfies $S(\mathcal{P}') = M$.*

Proof. Let v be an element of M. As $\pi_\mathfrak{m}(v) \in \pi_\mathfrak{m}(M) = S(\pi_\mathfrak{m}(B))$, there exists $a_i \in \mathcal{O}$ such that $v - \sum a_i C_i \in \mathfrak{m}\mathcal{O}^m$. Now the claim follows. □

Thus by computing a preimage $C = (c_{ij})$ of a strong echelon form over the ring $(\mathcal{O}/\mathfrak{m})$, we arrive at the following pseudomatrix spanning the original module (we write the coefficient

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

ideals in front of the corresponding rows):

$$\mathcal{P}' = \begin{array}{c} \mathcal{O} \\ \mathcal{O} \\ \mathcal{O} \\ \mathcal{O} \\ \mathcal{O} \\ \mathfrak{m} \\ \mathfrak{m} \\ \mathfrak{m} \\ \mathfrak{m} \\ \mathfrak{m} \end{array} \begin{pmatrix} c_{1,1} & & & & \\ * & c_{2,2} & & 0 & \\ * & * & \dots & & \\ * & * & \dots & \dots & \\ * & * & \dots & * & c_{m,m} \\ 1 & & & & \\ & 1 & & 0 & \\ & & \dots & & \\ & 0 & & \dots & \\ & & & & 1 \end{pmatrix}. \tag{4.2}$$

We now apply the classical pseudo-HNF algorithm of Cohen to this pseudomatrix. The special shape allows us to skip most of the steps and we actually never have to work with all of $\mathcal{P}'$.

ALGORITHM 5 (Demodularization). *Let $C \in \mathcal{O}^{m\times m}$ be a matrix such that $\pi_{\mathfrak{m}}(C)$ is a strong echelon form of $\pi_{\mathfrak{m}}(M)$. The following steps return a pseudo-HNF with span equal to M.*

(i) *For $i = m, \dots, 1$ do the following.*
(ii) *Let $\mathfrak{g} = (c_{i,i}, \mathfrak{m})$ and compute $x \in (c_{i,i})\mathfrak{g}^{-1}$, $y \in \mathfrak{m}\mathfrak{g}^{-1}$ such that $1 = x + y$.*
(iii) *Set $\mathfrak{b}_i = \mathfrak{g}$, $B_i = xA_i/c_{i,i}$ and $B_{i,i} = 1$.*
(iv) *Return $((\mathfrak{b}_i)_{1\leqslant i\leqslant m}, B)$.*

THEOREM 15. *Algorithm 5 is correct.*

Proof. For the proof it is convenient to think of all operations applied to the pseudomatrix $\mathcal{P}'$ in (4.2), which actually spans the module M by Lemma 14. We now take a look at Step (ii) and Step (iii). For the sake of convenience we consider only the case $i = m$. By [7, Proposition 1.3] the pseudomatrices

$$\begin{array}{c} (c_{m,m}) \\ \mathfrak{m} \end{array} \begin{pmatrix} c_{m,1}/c_{m,m} & \dots & c_{m,m-1}/c_{m,m} & 1 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

and

$$\begin{array}{c} \mathfrak{g} \\ \mathfrak{m}\mathfrak{g}^{-1} \end{array} \begin{pmatrix} x(c_{m,1}/c_{m,m}) & \dots & x(c_{m,m-1}/c_{m,m}) & 1 \\ -c_{m,1} & \dots & -c_{m,m-1} & 0 \end{pmatrix}$$

span the same module. We need to show that the second row of the latter pseudomatrix is superfluous. Let v be in the span of the second row. In particular $v \in S(M)$ and $\pi_{\mathfrak{m}}(v) \in \pi_{\mathfrak{m}}(M) = S(\pi_{\mathfrak{m}}(C))$. As the last entry is zero we have $\pi_{\mathfrak{m}}(v) \in S_1(\pi_{\mathfrak{m}}(C))$. As $\pi_{\mathfrak{m}}(C)$ is a strong echelon form this implies that there exists $r_j \in \mathcal{O}$ such that $v - \sum_{j=1}^{m-1} r_j C_j \in S_1(\mathfrak{m}\mathcal{O}^m)$. Thus $v = \sum_{j=1}^{m-1} r_j C_j + \sum_{j=1}^{m-1} s_j e_j$ for some $s_j \in \mathfrak{m}$ and $e_j = (\delta_{ji})_{1\leqslant i\leqslant m}$. □

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

A few remarks on the complexity. While the inversion of ideals requires at most $O(d^3)$ operations using a precomputed 2-element representation of the codifferent, the multiplication requires $O(d^4)$ operations if both ideals are given by their $\mathbf{Z}$-bases. Therefore a naive approach to Step (ii) requires $O(d^4)$ operations. But we can do better by noting that

$$\mathfrak{m}\mathfrak{g}^{-1} = (\mathfrak{m}(a)^{-1} \cap \mathcal{O}) \quad \text{and} \quad (a)\mathfrak{g}^{-1} = (\mathfrak{m}(a)^{-1} \cap \mathcal{O})^{-1} \cap \mathcal{O}.$$

Now the ideal product involves a principal ideal and can be performed using at most $O(d^3)$ operations. Since the artificially introduced inversions and intersections with $\mathcal{O}$ require at most $O(d^3)$ operations, the whole step requires at most $O(d^3)$ operations. Note that the naive application of the pseudo-HNF algorithm of Cohen would have required $O(n^2)$ operations similar to Step (ii) involving growing ideals. Let us summarize our algorithm.

ALGORITHM 6. *Given an $\mathcal{O}$-module M and a pseudomatrix $\mathcal{P}$ with $S(\mathcal{P}) = M$, the following steps return a pseudo-HNF of M.*

(i) *Find an ideal $\mathfrak{m}$ such that $\mathfrak{m}\mathcal{O}^m \subseteq M$ (see § 4.5).*
(ii) *Compute $C \in \mathcal{O}^{m\times m}$ such that $\pi_{\mathfrak{m}}(C)$ is a strong echelon form of $\pi_{\mathfrak{m}}(M)$ using Algorithms 3 and 7.*
(iii) *Return the result of Algorithm 5 applied to C.*

Let $\mathcal{P} = ((\mathfrak{a}_i), A)$ be a pseudomatrix with $A \in K^{n\times m}$ and span $M \subseteq \mathcal{O}^m$. Note that in order for the modular algorithm to be applicable, it is crucial that there exists some integral ideal $\mathfrak{m}$ such that $\mathfrak{m}\mathcal{O}^m \subseteq M \subseteq \mathcal{O}^m$, which is equivalent to A being of rank m. As in the case $\mathcal{O} = \mathbf{Z}$, without this assumption this modular technique will not work.

Now assume that $\mathcal{H} = ((\mathfrak{b}_i)_i, H)$ is a pseudo-HNF of $\mathcal{P}$. A transformation matrix from $\mathcal{P}$ to $\mathcal{H}$ is a matrix $U \in \mathrm{GL}_n(K)$ with $u_{ij} \in \mathfrak{b}_i\mathfrak{a}_j^{-1}$, $1 \leqslant i, j \leqslant n$, and $UA = H$. We note that our algorithm for computing a pseudo-HNF does not produce such a transformation. This is unsurprising, as the same problem can also be observed in the case of modular $\mathbf{Z}$-HNF algorithms, see for example [**11**]. In our algorithm, the problems already show up during the calculation over the quotient ring, since our strong echelon form algorithm does not compute a transformation matrix either. If needed, we can recover a transformation matrix U from $\mathcal{P}$ and $\mathcal{H}$ by solving linear systems of equations over K and by computing the kernel of A. The problem of computing a transformation matrix efficiently during the modular algorithm is open.

It is worthwhile mentioning the special case $\mathcal{O} = \mathbf{Z}$, for which we can recover the classical HNF over $\mathbf{Z}$. Let $M \subseteq \mathbf{Z}^m$ be a $\mathbf{Z}$-module of rank m with basis matrix $A \in \mathbf{Z}^{m\times m}$. Moreover let $d \in \mathbf{Z}_{>0}$ be an element with $d\mathbf{Z}^m \subseteq M$ and $C \in \mathbf{Z}^{m\times m}$ such that C modulo $d\mathbf{Z}$ is a strong echelon form of $\pi_d(M) \subseteq (\mathbf{Z}/d\mathbf{Z})^m$. Note that by multiplying the rows of C mod $d\mathbf{Z}$ with suitable elements of $(\mathbf{Z}/d\mathbf{Z})^\times$ and by adding suitable elements, we can achieve that the diagonal elements of C actually divide d. Thus the whole demodularization step is superfluous and C is the HNF of M. This is in total contrast to the classical modular HNF algorithms, where after a computation in $\mathbf{Z}/d\mathbf{Z}$ one again has to compute a non-modular HNF of a matrix similar to (4.2) (see [**11**, § 2.1]).

4.5. *Finding a modulus* $\mathfrak{m}$

The crucial step in our normal form algorithm is the existence of an integral ideal $\mathfrak{m}$ with $\mathfrak{m}\mathcal{O}^m \subseteq M$. While there are situations in which such an $\mathfrak{m}$ is readily available, for example when working with ideals in relative extensions of number fields, let us briefly sketch how to obtain such an $\mathfrak{m}$ in general.

First assume that $\mathcal{P} = ((\mathfrak{a}_i), A)$ is a pseudomatrix with $A \in K^{m\times m}$ and span equal to M. Then it is well known that the ideal $\mathfrak{d} = \det(A)\cdot\mathfrak{a}_1 \dots \mathfrak{a}_m \subseteq \mathcal{O}$ has the property that $\mathfrak{d}\mathcal{O}^m \subseteq M$.

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

Therefore it remains to show how to compute $\det(A)$ efficiently. By clearing denominators we may assume that A has only integral coefficients. Now a small primes modular algorithm can be used. Find enough rational primes p_i such that $\det(A)$ can be recovered from the determinant of A modulo $(\prod_i p_i)$. For each prime number compute the determinant of A modulo (p_i) using unimodular triangulation (Step (i) of Algorithm 3). Now use the Chinese remainder theorem to obtain $\det(A)$ modulo $(\prod_i p_i)$ and therefore $\det(A)$. We refer the reader to [4] for details on the required size of $(\prod_i p_i)$.

Now consider the general case with $A \in K^{n\times m}$, $n \geqslant m$. In [8, Definition 1.4.9] the notion of *minor ideals* of pseudomatrices is introduced, which is a natural extension of minors to pseudomatrices (instead of extracting only rows and columns one also has to take care of the coefficient ideals). Moreover it is shown that the *determinantal ideal* $\mathfrak{d} \subseteq \mathcal{O}$ of $\mathcal{P}$, which is defined to be the sum of all $m \times m$ minor ideals of $\mathcal{P}$, satisfies $\mathfrak{d}\mathcal{O}^m \subseteq M$. Note that since in general there are just too many minor ideals (as in the case of minors of matrices), in order to find an ideal $\mathfrak{m}$ with $\mathfrak{m}\mathcal{O}^m \subseteq M$ it is sufficient to compute only *one* non-zero minor ideal (which exists since M has rank m).

5. *Splitting the modulus*

In order to speed up computations, we would like, if possible, to split the modulus, the idea being that if $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$, then, by the Chinese remainder theorem, $(\mathcal{O}/\mathfrak{m}) = (\mathcal{O}/\mathfrak{a}) \times (\mathcal{O}/\mathfrak{b})$ and thus 'everything' modulo $\mathfrak{m}$ can be done more efficiently by computing in $(\mathcal{O}/\mathfrak{a})$ and $(\mathcal{O}/\mathfrak{b})$. If we allow for a complete factorization, we of course achieve $(\mathcal{O}/\mathfrak{m}) = \prod_{\mathfrak{p}}(\mathcal{O}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})$, however, for general $\mathfrak{m}$, a factorization is prohibitively expensive. We observe that the complete factorization would result in the best complexity!

Furthermore, for any prime $\mathfrak{p}$ of degree one we have

$$(\mathcal{O}/\mathfrak{p}^k) \cong \mathbf{Z}/p^k\mathbf{Z}$$

for p the rational prime with $\mathfrak{p} \cap \mathbf{Z} = (p)$. Again, the Chinese remainder theorem, this time for $\mathbf{Z}$, allows us to combine any degree one prime ideals with distinct underlying rational primes into one, thus obtaining

$$(\mathcal{O}/\mathfrak{m}) \cong (\mathbf{Z}/m\mathbf{Z}) \times (\mathcal{O}/\mathfrak{m}')$$

with some potentially much smaller ideal $\mathfrak{m}'$. Once such a decomposition is obtained, much faster algorithms for $\mathbf{Z}/m\mathbf{Z}$ can be applied for hopefully a large part of the ring.

Unfortunately, without the use of factorization such a complete splitting is difficult to achieve. We propose the following simple algorithm, which is aimed at computing a large portion of the 'degree one part' while still being fast.

ALGORITHM 7 ($\mathbf{Z}$-split). *Let $\mathfrak{m}$ be an integral ideal. The following steps will produce coprime integral ideals $\mathfrak{a}$, $\mathfrak{b}$ with $\mathfrak{a}\mathfrak{b} = \mathfrak{m}$ and a rational integer $m \in \mathbf{Z}$ such that $(\mathcal{O}/\mathfrak{a}) \cong \mathbf{Z}/m\mathbf{Z}$.*

(i) *Let $m = \min(\mathbf{Z}_{\geqslant 1} \cap \mathfrak{m})$ and $b = \mathbf{N}(\mathfrak{m})/m$.*
(ii) *Repeat*
(iii) *compute $g = \gcd(m, b)$, $m = m/g$ and $b = b^2 \bmod m$,*
(iv) *until $g = 1$.*
(v) *Compute $\mathfrak{a} = m\mathcal{O} + \mathfrak{m}$ and $\mathfrak{b} = (\mathbf{N}(\mathfrak{m})/m)\mathcal{O} + \mathfrak{m}$.*
(vi) *Return $\mathfrak{a}, \mathfrak{b}$.*

Note that this algorithm will not necessarily find a maximal ideal $\mathfrak{a} \mid \mathfrak{m}$ such that $(\mathcal{O}/\mathfrak{a}) \cong \mathbf{Z}/m\mathbf{Z}$ and $\mathfrak{a}$, $\mathfrak{m}\mathfrak{a}^{-1}$ are coprime. Let $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}_1\mathfrak{q}_2$ where $\mathfrak{p}_i$, $\mathfrak{q}_i$ are primes of degree one lying above distinct rational primes p and q respectively. Then $\min(\mathfrak{m}) = pq$ and $\mathbf{N}(\mathfrak{m}) = p^2q^2$, so

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

the algorithm will terminate with $\mathfrak{a} = \mathcal{O}$. However, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{q}_1$ would be a correct result, but we need to actually factorize $\mathfrak{m}$ to find this decomposition.

Proof of correctness. For any integral ideal $\mathfrak{a}$ the minimum $\min(\mathfrak{a}) = \min(\mathbf{Z}_{\geqslant 1} \cap \mathfrak{a})$ is equal to $\exp(\mathcal{O}/\mathfrak{a})$ (the exponent of the abelian group $(\mathcal{O}/\mathfrak{a})$). Clearly, $\min(\mathfrak{a}) \in \mathfrak{a}$ and $\mathrm{ord}(1) = \min \mathfrak{a}$ where ord is the order of the element. Thus if $\mathbf{N}(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}| = \min(\mathfrak{a})$, then $(\mathcal{O}/\mathfrak{a}) \cong \mathbf{Z}/\min(\mathfrak{a})\mathbf{Z}$, generated by 1.

From the decomposition above we see that if $\mathbf{N}(\mathfrak{a}) \neq \min(\mathfrak{a})$, then we either have a prime $\mathfrak{q}$ dividing $\mathfrak{a}$ of degree greater then one, we have at least two distinct prime ideals $\mathfrak{q}_i \mid \mathfrak{a}$ $(i = 1, 2)$ lying above the same rational prime or we have some ramified prime $\mathfrak{q}$ with $\mathfrak{q}^2 \mid \mathfrak{a}$. In the first case $(\mathcal{O}/\mathfrak{q}, +)$ is a non-cyclic group, in the second case we have a product of two cyclic groups with non-coprime orders while in the last case clearly $\min(\mathfrak{q}) = \min(\mathfrak{q}^2)$, but $\mathbf{N}(\mathfrak{q}) \neq \mathbf{N}(\mathfrak{q}^2)$. In all other cases $\mathfrak{a}$ is composed of powers of degree one prime ideals over distinct rational primes as well as ramified primes with exponent 1.

In the algorithm b initially contains all rational primes q such that either $\mathfrak{q} \mid q$ for some prime of degree greater then one, $\mathfrak{q}_i \mid q$ with $i = 1, 2$ or $\mathfrak{q}^2 \mid \mathfrak{a}$ for some ramified prime $\mathfrak{q} \mid q$. During the loop, we remove all those rational primes from m and in the final step we then split $\mathfrak{m}$ accordingly. The squaring of b ensures that the total time is polynomially bounded. □

Let $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$ be the splitting obtained by this algorithm. Experimentally, we have $\mathbf{N}(\mathfrak{b}) \ll \mathbf{N}(\mathfrak{a})$, in fact frequently, $\mathbf{N}(\mathfrak{b}) = 1$, thus the effort to compute a pseudo-HNF over a number field is mostly independent of its degree and depends almost *only* on the dimension of the matrix.

We note that the CRT techniques for the HNF are also used to derive (expected) polynomial complexity in the presence of lots of small prime ideals: the runtime depends on $p_{\mathfrak{m}}$ and $p_{\mathfrak{m}}$ is mainly determined by the norms of the small prime ideals. Thus we use the approach of Belabas (see [2, § 6]) to split the modulus into small primes, where we can directly use his (deterministic) linear algebra approach to find uniformizing elements and thus work in the completions. For the (large) remainder term, we use our randomized methods.

6. *Computations*

We have implemented both the Euclidean structure and the improved pseudo-HNF computation in the computer algebra system Magma [5]. To illustrate the efficiency of our techniques, we computed pseudo-HNFs for random matrices over a range of fields. In particular, we used $K = \mathbf{Q}[t]/(t^d - 10)$ for $d = 2$, 4, 8, and generated matrices of dimensions n up to 300, depending on d. More specifically, starting at $k = 1$, we computed for two random matrices A of dimension $n = 10 \cdot k$ a pseudo-HNF of the pseudomatrix $((\mathcal{O})_{1 \leqslant i \leqslant n}, A)$ both using our method and Magma's implementation of Cohen's algorithm (available through the command HermiteForm) until a single computation took more than one hour. By random matrices we mean matrices over $\mathcal{O}$, where the coefficients (with respect to a fixed integral basis) of the matrix entries are chosen uniformly in $\{-2^B, \ldots, 2^B\}$ for the times t_1, t_2 and rounded normally distributed with mean 0 and variance 2^{2B} for the times g_1, g_2. Table 1 shows the results for different choices of parameters d, n and B, where t_1 (respectively g_1) denotes the running time (in seconds) using Algorithm 6 and t_2 (respectively g_2) the running time (in seconds) using Magma's implementation of Cohen's algorithm. We briefly note that the longer running times for the normal distributed matrix entries are a consequence of them being larger: by Hadamard's inequality, the size of the determinant depends mainly on the largest entry in each row or column respectively. Using normal distributed entries, this maximum value will usually be larger than 2^B, which is reflected in the runtime.

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

7. *Conclusions*

In the preceding sections, we presented a suite of new algorithms to explicitly utilize the Euclidean structure of quotients of rings of integers. The power of those ideas was demonstrated via a new, probabilistic, modular algorithm to compute normal forms of modules over rings of integers. The resulting algorithm is both faster and conceptually simpler as it does not need to work with the pseudobases and the coefficient ideals.

Our new lifting algorithm to obtain a non-modular Hermite form is even in the case of $\mathbf{Z}$-modules new and conceptually simpler than the usual lifting algorithm: we do not need to perform any elimination steps in characteristic 0, all is done through the adapted Howell normal form on the modular 'side'.

While we did not do a complete bit complexity analysis for the pseudo Hermite normal form algorithm (Algorithm 6), it is clear that the method presented has polynomial expected complexity: the modular algorithms all use an expected polynomial number of operations on elements of a bounded size and the lifting steps are easily realized using linear algebra over $\mathbf{Z}$. The comparison with Cohen's algorithm on theoretical grounds is difficult as his algorithm is not analyzed and conjectured to have exponential runtime due to intermediate coefficient swell. A suitably modified modular version was proven to be polynomial time in [3], but while the complexity in the module dimension is the same, the complexity in the field degree is far worse there due to the expensive ideal operations, in particular the lattice basis reduction to keep the ideals bounded in size.

Future work will try to find faster and deterministic algorithms.

TABLE 1. *Algorithm 6 versus* MAGMA*'s HermiteForm.*

d	B	n	t_1	t_2	t_2/t_1	g_1	g_2	g_2/g_1
2	10	10	0.095	0.020	0.210	0.030	0.010	0.333
		20	0.130	0.065	0.500	0.335	0.080	0.238
		30	0.375	0.210	0.560	0.465	0.155	0.333
		40	0.325	0.300	0.923	0.405	0.360	0.888
		200	107.715	143.975	1.336	128.335	165.475	1.289
		300	580.370	1031.430	1.777	842.675	1210.775	1.436
2	100	10	0.075	0.155	2.066	0.055	0.090	1.636
		20	0.380	0.655	1.723	0.400	0.740	1.850
		30	1.245	2.490	2.000	1.455	2.890	1.986
		40	3.265	6.985	2.139	3.155	10.630	3.369
		80	47.945	107.115	2.234	51.495	107.320	2.084
		140	549.080	1194.445	2.175	540.660	1008.665	1.865
4	10	10	0.080	0.055	0.687	0.055	0.085	1.545
		20	0.260	0.390	1.500	0.195	0.385	1.974
		30	0.525	1.040	1.980	0.640	1.325	2.070
		40	1.955	3.080	1.575	0.945	3.440	3.640
		80	10.080	37.970	3.515	12.165	48.505	3.987
		140	77.640	346.315	4.460	107.005	402.735	3.763
8	10	10	0.290	0.850	2.931	0.160	0.660	4.125
		20	0.620	5.345	8.620	1.445	6.955	4.813
		30	1.605	26.470	16.492	1.785	33.190	18.593
		40	5.675	57.535	10.138	7.355	96.797	13.160
		80	48.445	746.120	15.401	44.720	917.765	20.522

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press

References

1. A. G. Ağargün and C. R. Fletcher, 'Euclidean rings', *Turkish J. Math.* 19 (1995) no. 3, 291–299.
2. K. Belabas, 'Topics in computational algebraic number theory', *J. Théor. Nombres Bordeaux* 16 (2004) no. 1, 19–63.
3. J.-F. Biasse and C. Fieker, 'A polynomial time algorithm for computing the HNF of a module over the integers of a number field', *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation (ISSAC '12)* (ACM, New York, NY, USA, 2012) 75–82.
4. J.-F. Biasse, C. Fieker and T. Hofmann, 'On the computation of the HNF of a module over the ring of integers of a number field', *J. Symbolic Comput.*, submitted.
5. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) no. 3–4, 235–265; Computational algebra and number theory (London, 1993).
6. W. Bosma and M. Pohst, 'Computations with finitely generated modules over Dedekind rings', *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation (ISSAC '91)* (ACM, New York, NY, USA, 1991) 151–156.
7. H. Cohen, 'Hermite and Smith normal form algorithms over Dedekind domains', *Math. Comp.* 65 (1996) no. 216, 1681–1699.
8. H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics 193 (Springer, New York, 2000).
9. P. D. Domich, R. Kannan and L. E. Trotter Jr, 'Hermite normal form computation using modulo determinant arithmetic', *Math. Oper. Res.* 12 (1987) no. 1, 50–59.
10. C. R. Fletcher, 'Euclidean rings', *J. Lond. Math. Soc.* (2) 4 (1971) 79–82.
11. J. L. Hafner and K. S. McCurley, 'Asymptotically fast triangularization of matrices over rings', *SIAM J. Comput.* 20 (1991) no. 6, 1068–1083.
12. J. A. Howell, 'Spans in the module $(Z_m)^s$', *Linear Multilinear Algebra* 19 (1986) no. 1, 67–77.
13. C. S. Iliopoulos, 'Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrix', *SIAM J. Comput.* 18 (1989) no. 4, 658–669.
14. E. Steinitz, 'Rechteckige Systeme und Moduln in algebraischen Zahlköppern. I', *Math. Ann.* 71 (1911) no. 3, 328–354.
15. E. Steinitz, 'Rechteckige Systeme und Moduln in algebraischen Zahlkörpern. II', *Math. Ann.* 72 (1912) no. 3, 297–345.
16. A. Storjohann, 'Algorithms for matrix canonical forms', PhD Thesis, Department of Computer Science, Swiss Federal Institute of Technology – ETH, 2000.
17. A. Storjohann and T. Mulders, 'Fast algorithms for linear algebra modulo N', *Algorithms — ESA '98 (Venice)*, Lecture Notes in Computer Science 1461 (Springer, Berlin, 1998) 139–150.

Claus Fieker
Fachbereich Mathematik
Technische Universität Kaiserslautern
Postfach 3049, 67653 Kaiserslautern
Germany

fieker@mathematik.uni-kl.de

Tommy Hofmann
Fachbereich Mathematik
Technische Universität Kaiserslautern
Postfach 3049, 67653 Kaiserslautern
Germany

thofmann@mathematik.uni-kl.de

https://doi.org/10.1112/S1461157014000291 Published online by Cambridge University Press