International Journal of Pure and Applied Mathematics

Volume 16 No. 2 2004, 241-249

ON THE STRUCTURE OF THE RING $\mathbb{Z}\left[\sqrt[3]{2}\right]$

Bram van Asch

Department of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, THE NETHERLANDS
e-mail: a.g.v.asch@tue.nl

Abstract: It has been known for some time that the ring $\mathbb{Z}\left[\sqrt[3]{2}\right]$ is Euclidean. The first one to prove this fact in a general setting was H.J. Godwin (see [4]). In this note we present an explicit description of the Euclidean algorithm in this ring. Besides, all primes in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ are determined.

AMS Subject Classification: 11R04, 11R16, 11R27
Key Words: ring of integers, division algorithm, prime

1. Introduction

In the ring $\mathbb{Z}$ the following property is well-known: given integers a and b, with $b \neq 0$, there exist integers q and r such that $a = qb + r$ and $0 \leq r < |b|$. This is called the Euclidean property of this ring. It is used for instance in the Euclidean algorithm, a very efficient way to determine the greatest common divisor of two integers. More general an Euclidean ring is a commutative ring R where a map $N : R \to \mathbb{N} \cup \{0\}$ is defined such that for all $\alpha, \beta \in R$ there are $\omega, \rho \in R$ with $\alpha = \omega\beta + \rho$ and $N(\rho) < N(\beta)$. Many examples occur in algebraic number theory. If K is some finite-dimensional extension of $\mathbb{Q}$ we can consider the ring R of algebraic integers. In many cases this yields an

Received: August 12, 2004

Euclidean ring. For instance the ring $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$ of Gaussian integers, with $N(a+bi) = a^2+b^2$. In fact it is easy to determine the ring of algebraic integers in an arbitrary quadratic number field $\mathbb{Q}\left(\sqrt{d}\right)$: $R = \mathbb{Z}\left[\sqrt{d}\right]$ when $d \equiv 2 \bmod 4$ or $d \equiv 3 \bmod 4$ and $R = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ when $d \equiv 1 \bmod 4$. There is a complete list of values for d for which these rings of integers are Euclidean, see [1]. For cubic number fields the situation is different, i.e. there is no complete list of Euclidean rings of integers in this case. The most simple case is $\mathbb{Q}\left(\sqrt[3]{2}\right)$. It is not hard to prove that the ring of algebraic integers is given by $\mathbb{Z}\left[\sqrt[3]{2}\right] = \left\{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c \in \mathbb{Z}\right\}$ (see for instance [3]). In [7] this ring is used to describe a factoring method for numbers of the form x^3+2. Besides the question is asked there whether an Euclidean algorithm does exist in this ring. The affirmative answer to this question can be found for instance in [4]. We also refer to [2], where all norm-Euclidean cubic number fields with discriminants $-999 < d < 10^4$ are listed. In [2] the authors use computerprograms to compute so-called Euclidean minima, which enables them to decide that rings of integers in certain cubic number fields are Euclidean. In this paper it will be proved by hand that the ring $\mathbb{Z}\left[\sqrt[3]{2}\right]$ is Euclidean. The proof is constructive, i.e. it yields an explicit description of the division algorithm. As a consequence all nonzero non-unit elements in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ can be factorized as a product of primes. In a certain sense this factorization is unique. Primes in a number field occur as decompositions of rational primes. In [3] a general description of the splitting of rational primes in cubic number fields can be found. In Section 4. we give an explicit description of all primes in $\mathbb{Z}\left[\sqrt[3]{2}\right]$, using the Euclidean algorithm.

2. Notation

There are three embeddings of $\mathbb{Q}\left(\sqrt[3]{2}\right)$ into the field $\mathbb{C}$ of complex numbers:

$$\chi_1\left(a+b\sqrt[3]{2}+c\sqrt[3]{4}\right) = a+b\sqrt[3]{2}+c\sqrt[3]{4},$$

$$\chi_2\left(a+b\sqrt[3]{2}+c\sqrt[3]{4}\right) = a+b\zeta\sqrt[3]{2}+c\zeta^2\sqrt[3]{4},$$

$$\chi_3\left(a+b\sqrt[3]{2}+c\sqrt[3]{4}\right) = a+b\zeta^2\sqrt[3]{2}+c\zeta\sqrt[3]{4},$$

where $\zeta = e^{\frac{2\pi i}{3}}$. For $\alpha = a+b\sqrt[3]{2}+c\sqrt[3]{4} \in \mathbb{Q}\left(\sqrt[3]{2}\right)$ we put $\overline{\alpha} = \chi_2(\alpha)\,\chi_3(\alpha) \in \mathbb{Q}\left(\sqrt[3]{2}\right)$. If $\alpha \in \mathbb{Z}\left[\sqrt[3]{2}\right]$ then $\overline{\alpha} \in \mathbb{Z}\left[\sqrt[3]{2}\right]$, too. The Galois-norm on $\mathbb{Q}\left(\sqrt[3]{2}\right)$ is

defined by $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} = F(a,b,c)$, where $F(a,b,c) = a^3 + 2b^3 + 4c^3 - 6abc$. And finally we put $N(\alpha) = \left|N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\alpha)\right|$.

3. The Division Algorithm

From the definition of the norm N the following properties are obvious.

Proposition 1. *1.* $N(\alpha) = 0$ *if and only if* $\alpha = 0$.
2. $N(\alpha\beta) = N(\alpha)N(\beta)$.

The following properties of the function F are the basis for the division algorithm.

Proposition 2. *Consider the function* F *on the domain* $-\frac{1}{2} \le u, v, w \le \frac{1}{2}$. *The following properties hold:*

i. $F(-u,-v,-w) = -F(u,v,w)$.
ii. If u *and* v *have the same sign then* $|F(u,v,w)| < 1$.
iii. If $u \le 0,\ v,w \ge 0$ *and* $|F(u,v,w)| \ge 1$ *then* $|F(u+1,v,w)| < 1$.
iv. If $u,w \ge 0,\ v \le 0$ *and* $|F(u,v,w)| \ge 1$ *then* $|F(u,v+1,w)| < 1$.
v. If $u \ge 0,\ v,w \le 0$ *and* $|F(u,v,w)| \ge 1$ *then* $|F(u-1,v,w)| < 1$.
vi. If $u,w \le 0,\ v \ge 0$ *and* $|F(u,v,w)| \ge 1$ *then* $|F(u,v-1,w)| < 1$.

Proof. i. Trivial.

ii. In view of (i) we only need to consider the case $u, v \ge 0$. If $u,v,w \ge 0$ then $-\frac{3}{4} \le F(u,v,w) \le \frac{7}{8}$. If $u,v \ge 0$ and $w \le 0$ then $-\frac{1}{2} \le F(u,v,w) \le \frac{3}{8} + 4w^3 - \frac{3}{2}w < \frac{3}{4}$.

iii. For $u \le 0,\ v,w \ge 0$ we have $F(u,v,w) \ge -\frac{1}{8}$ so we only have to consider the possibility that $F(u,v,w) \ge 1$. If $-\frac{1}{6} \le u \le 0$ then we have $F(u,v,w) < 1$. So let $-\frac{1}{2} \le u \le -\frac{1}{6}$. If we consider $F(u,v,w)$ only as a function of the negative variable u it has its absolute maximum value if $\frac{\partial F}{\partial u} = 0$, i.e. if $u = -\sqrt{2vw}$. This maximum value is equal to $2v^3 + 4w^3 + 4\sqrt{2}(vw)^{\frac{3}{2}}$. Now it is easy to check that if $0 \le v \le 0.34$ (and $0 \le w \le \frac{1}{2}$) or $0 \le w \le 0.39$ (and $0 \le v \le \frac{1}{2}$) we have $2v^3+4w^3+4\sqrt{2}(vw)^{\frac{3}{2}} < 1$. So $F(u,v,w) > 1$ can only occur if $v \ge 0.34$ and $w \ge 0.39$. The value of $-\sqrt{2vw}$ is now outside the interval $\left[-\frac{1}{2}, -\frac{1}{6}\right]$ and therefore $F(u,v,w)$ has its maximum value for $u = -\frac{1}{2}$. Then we have $F(u,v,w) \le -\frac{1}{8} + 2v^3 + 4w^3 + 3vw \le \frac{11}{8}$. Suppose now furthermore that $vw \le 0.16$. Then we have $F(u,v,w) \le -\frac{1}{8} + 2v^3 + 4w^3 + 0.48 \le 0.36 + 2v^3 + 4\left(\frac{0.16}{v}\right)^3$. Now $w \ge 0.39$ and $vw \le 0.16$ imply $v \le 0.42$. It is easy to check that $0.36 + 2v^3 + 4\left(\frac{0.16}{v}\right)^3 < 1$ for $0.34 \le v \le 0.42$. So we conclude that $F(u,v,w) \ge 1$ can occur only if

$v \geq 0.34,\ w \geq 0.39$ and $vw > 0.16$. If $F(u,v,w) \geq 1$ we replace u by $u+1$ and we remark that $F(u+1,v,w) = F(u,v,w) + 3u^2 + 3u + 1 - 6vw$. With the given limits for u and vw we have $-1.25 \leq 3u^2 + 3u + 1 - 6vw \leq -0.376$. Together with $1 \leq F(u,v,w) \leq 1.375$ this proves that $|F(u+1,v,w)| < 1$.

iv. Again we only have to consider the possibility that $F(u,v,w) \geq 1$. For $-\frac{1}{4} \leq v \leq 0$ we have $F(u,v,w) < 1$, so let $-\frac{1}{2} \leq v \leq -\frac{1}{4}$. We consider $F(u,v,w)$ as a function of the negative variable v. This function has its maximum value $u^3+4w^3+4(uw)^{\frac{3}{2}}$ at $v = -\sqrt{uw}$. For $u \leq 0.44$ (and $0 \leq w \leq \frac{1}{2}$) or $w \leq 0.47$ (and $0 \leq u \leq \frac{1}{2}$) we have $u^3 + 4w^3 + 4(uw)^{\frac{3}{2}} < 1$. Suppose now that $u \geq 0.44,\ w \geq 0.47$ and $F(u,v,w) \geq 1$. Still we have $F(u,v,w) \leq u^3 + 4w^3 + 4(uw)^{\frac{3}{2}} \leq \frac{9}{8}$. Besides $F(u,v+1,w) = F(u,v,w) + 6v^2 + 6v + 2 - 6uw$. With the given limits for u, v and w one easily checks that $-1 \leq 6v^2 + 6v + 2 - 6uw \leq -0.36$. This proves that $|F(u,v+1,w)| < 1$.

v. Follows from (i) and (iii).

vi. Follows from (i) and (iv). □

Proposition 3. *For all $\alpha, \beta \in \mathbb{Z}\left[\sqrt[3]{2}\right]$, $\beta \neq 0$ there are $\omega, \rho \in \mathbb{Z}\left[\sqrt[3]{2}\right]$ such that $\alpha = \omega\beta + \rho$ and $N(\rho) < N(\beta)$.*

Proof. Let $\alpha, \beta \in \mathbb{Z}\left[\sqrt[3]{2}\right],\ \beta \neq 0$. Then

$$\frac{\alpha}{\beta} = \frac{1}{\beta\overline{\beta}}\left(\overline{\beta}\alpha\right) = q_1 + q_2\sqrt[3]{2} + q_3\sqrt[3]{4} \in \mathbb{Q}\left(\sqrt[3]{2}\right).$$

Next determine unique integers v_i such that $-\frac{1}{2} \leq q_i - v_i < \frac{1}{2}$: $v_i = \left\lfloor q_i + \frac{1}{2} \right\rfloor$, where $\lfloor . \rfloor$ denotes the greatest integer function. If

$$N\left((q_1 - v_1) + (q_2 - v_2)\sqrt[3]{2} + (q_3 - v_3)\sqrt[3]{4}\right) < 1,$$

then we put $\omega = v_1 + v_2\sqrt[3]{2} + v_3\sqrt[3]{4}$. If

$$N\left((q_1 - v_1) + (q_2 - v_2)\sqrt[3]{2} + (q_3 - v_3)\sqrt[3]{4}\right) \geq 1,$$

then one of the $q_i - v_i$ must have a sign different from the other two. Put in this case $w_i = v_i \pm 1,\ w_j = v_j$ for $i \neq j$, and $\omega = w_1 + w_2\sqrt[3]{2} + w_3\sqrt[3]{4}$, such that, according to Proposition 2

$$N\left((q_1 - w_1) + (q_2 - w_2)\sqrt[3]{2} + (q_3 - w_3)\sqrt[3]{4}\right) < 1.$$

In each case therefore we can find $\omega \in \mathbb{Z}\left[\sqrt[3]{2}\right]$ such that $N\left(\frac{\alpha}{\beta} - \omega\right) < 1$. By putting $\rho = \alpha - \omega\beta$ we get $\alpha = \omega\beta + \rho$, and $N(\rho) < N(\beta)$. □

Example 1. Let $\alpha = 180 + 157\sqrt[3]{2} + 274\sqrt[3]{4}$ and $\beta = 11 - 7\sqrt[3]{2} + 13\sqrt[3]{4}$. Then $\frac{\alpha}{\beta} = \frac{252444}{15439} + \frac{70759}{15439}\sqrt[3]{2} + \frac{131257}{15439}\sqrt[3]{4}$, so $v_1 = 16,\ v_2 = 5,\ v_3 = 9$. In this case we have $N\left((q_1 - v_1) + (q_2 - v_2)\sqrt[3]{2} + (q_3 - v_3)\sqrt[3]{4}\right) = \frac{15968}{15439} > 1$. Put $w_1 = v_1 + 1 = 17,\ w_2 = v_2 = 5,\ w_3 = v_3 = 9$ and $\omega = 17 + 5\sqrt[3]{2} + 9\sqrt[3]{4}$. Then we have $\alpha = \omega\beta + \rho$, where $\rho = \alpha - \omega\beta = -11 - 13\sqrt[3]{2} - 11\sqrt[3]{4}$ and $N(\rho) = 1611 < N(\beta) = 15439$.

The existence of this division algorithm implies that $\mathbb{Z}\left[\sqrt[3]{2}\right]$ is a principal ideal domain. For all $\alpha, \beta \in \mathbb{Z}\left[\sqrt[3]{2}\right]$ the greatest common divisor $\gcd(\alpha, \beta)$ exists and it can be determined in an efficient way by the Euclidean algorithm. Besides every nonzero non-unit is a product of primes.

4. Primes in $\mathbb{Z}\left[\sqrt[3]{2}\right]$

The factorization of elements in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ is unique in the following sense. Let S be a set of primes in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ such that

i. every prime in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ is associate to a prime in S,

ii. no two primes in S are associate.

Then for every nonzero $\alpha \in \mathbb{Z}\left[\sqrt[3]{2}\right]$ we have $\alpha = \mu \prod_{\pi \in S} \pi^{e(\pi)}$, where μ is a unit, $e(\pi) \geq 0$ and $e(\pi) = 0$ for almost all π. For a given α the unit μ and the exponents $e(\pi)$ are uniquely determined. The concepts of associated elements and primes are defined as follows.

Definition 1. Two elements $\alpha, \beta \in \mathbb{Z}\left[\sqrt[3]{2}\right]$ are called associate if $\alpha = \mu\beta$ for some unit μ. An element $\pi \in \mathbb{Z}\left[\sqrt[3]{2}\right]$, $\pi \neq 0$, which is not a unit, and has only units and associate elements as divisors, is called a prime in $\mathbb{Z}\left[\sqrt[3]{2}\right]$.

There are infinitely many units in $\mathbb{Z}\left[\sqrt[3]{2}\right]$, so for every element there are infinitely many associated elements. The group of units is described in the following proposition, which is a special case of the Dirichlet Units Theorem (see for instance [8], Theorem 12.6).

Proposition 4. *The group of units in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ is the direct product of $\{\pm 1\}$ and $\left\langle \sqrt[3]{2} - 1 \right\rangle$, the cyclic group generated by $\sqrt[3]{2} - 1$.*

The next proposition follows immediately from Proposition 1(ii).

Proposition 5. *If for $\pi \in \mathbb{Z}\left[\sqrt[3]{2}\right]$ the norm $N(\pi)$ is a rational prime, then π is a prime in $\mathbb{Z}\left[\sqrt[3]{2}\right]$.*

Example 2. Since $N\left(\sqrt[3]{2}\right) = 2$ the element $\sqrt[3]{2}$ is a prime. The element $1 + \sqrt[3]{2}$ is a prime with norm equal to 3. In fact, as we will see later, every prime in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ with norm equal to 3 is associated to $1 + \sqrt[3]{2}$.

Proposition 6. *For all primes π in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ there is a rational prime p such that $\pi|p$.*

Proof. We have $N(\pi) = |\pi\overline{\pi}|$ and $N(\pi)$ being a rational integer we also have $N(\pi) = p_1...p_t$ for some rational primes $p_1, ..., p_t$. Therefore $\pi\overline{\pi} = \pm p_1...p_t$. And since π is a prime we conclude $\pi|p_i$ for some p_i. □

So when we are looking for primes in the ring $\mathbb{Z}\left[\sqrt[3]{2}\right]$ it suffices to consider divisors of rational primes. To analyse this further we use [6], p. 27, Proposition 25, which reads in this case as follows. Let p be a rational prime and let $f(x) = x^3 - 2$. Let $\overline{f}(x)$ denote the reduction of $f(x)$ modulo p. Factorize $\overline{f}(x)$ into monic irreducible polynomials: $\overline{f}(x) = \overline{f}_1^{e_1}(x)\overline{f}_2^{e_2}(x)\overline{f}_3^{e_3}(x)$, where $e_i = 0$ or $e_i = 1$. Let $f_i(x)$ be some monic polynomial in $\mathbb{Z}[x]$ such that its reduction modulo p is equal to $\overline{f}_i(x)$. Then we have $p\mathbb{Z}\left[\sqrt[3]{2}\right] = P_1^{e_1}P_2^{e_2}P_3^{e_3}$ and the ideals P_i in $\mathbb{Z}\left[\sqrt[3]{2}\right]$ are given by $P_i = p\mathbb{Z}\left[\sqrt[3]{2}\right] + f_i\left(\sqrt[3]{2}\right)\mathbb{Z}\left[\sqrt[3]{2}\right]$. The ring $\mathbb{Z}\left[\sqrt[3]{2}\right]$ is a principal ideal domain, and therefore we can write $P_i = \pi_i\mathbb{Z}\left[\sqrt[3]{2}\right]$ for some prime $\pi_i = \gcd\left(p, f\left(\sqrt[3]{2}\right)\right)$. In this way we can determine prime divisors of p.

Suppose p is an odd rational prime. We consider three cases:

1. $p = 3$

In $\mathbb{Z}_3[x]$ we have $x^3 - 2 = (x-2)^3$, and therefore 3 has up to unit factors only one prime divisor, for instance $\pi = 1 + \sqrt[3]{2}$.

2. $p \equiv 2 \bmod 3$.

Let g be a generator of $\mathbb{Z}_p^*$. Since $\gcd(p-1, 3) = 1$ the element g^3 is also a generator. So we can find a unique integer k, $0 < k \leq p-1$, such that $\left(g^3\right)^k = 1$, which can also be written as $\left(g^k\right)^3 = 2$. Therefore the equation $x^3 - 2 = 0$ has a unique solution $a = g^k$ in $\mathbb{Z}_p$, and as a consequence the polynomial $x^3 - 2$ factorizes in $\mathbb{Z}_p[x]$ as $x^3 - 2 = (x-a)g(x)$ for some irreducible quadratic polynomial $g(x)$. Next we consider both $x - a$ and $g(x)$ as polynomials in $\mathbb{Z}[x]$, and determine $\gcd(p, \sqrt[3]{2} - a)$ and $\gcd\left(p, g\left(\sqrt[3]{2}\right)\right)$. This yields prime divisors π_1 and π_2 of p. Their norms are equal to p and p^2.

3. $p \equiv 1 \bmod 3$.

The situation is different in this case. The equation $x^3 - 2 = 0$ has a solution in $\mathbb{Z}_p$, i.e. 2 is a cubic residue modulo p, if and only if $p = m^2 + 27n^2$ for some integers a, b (see for instance [5], Proposition 9.6.2). In that case there are three solutions since $\mathbb{Z}_p$ contains the three cubic roots of unity. So $\overline{f}(x) = x^3 - 2$ is in $\mathbb{Z}_p[x]$ a product of three linear factors, $\overline{f}(x) = (x - a_1)(x - a_2)(x - a_3)$.

By the same procedure as in 2. We find in this way three prime divisors $\pi_i = \gcd\left(p, \sqrt[3]{2} - a_i\right), i = 1, 2, 3$, of p. If p is not a cubic residue modulo p then $x^3 - 2$ is irreducible in $\mathbb{Z}_p[x]$. In this case p does not split in $\mathbb{Z}\left[\sqrt[3]{2}\right]$, i.e. p is also prime in $\mathbb{Z}\left[\sqrt[3]{2}\right]$.

Summarizing we get the following proposition.

Proposition 7. *i.* $\sqrt[3]{2}$ *is up to unit factors the only prime with norm equal to 2.*

ii. $1 + \sqrt[3]{2}$ *is up to unit factors the only prime with norm equal to 3.*

iii. Every rational prime p *with* $p \equiv 2$ *mod* 3 *splits as a product* $p = \pi_1\pi_2$ *of primes such that* $N(\pi_1) = p$ *and* $N(\pi_2) = p^2$.

iv. Every rational prime p *with* $p \equiv 1$ *mod* 3 *and* $p = m^2 + 27n^2$ *for some integers* m, n *splits as a product* $p = \pi_1\pi_2\pi_3$ *of three non-associated primes, all with norm equal to* p.

v. If p *is a rational prime with* $p \equiv 1$ *mod* 3 *and* p *is not a cubic residue modulo* p *then* p *is also a prime in* $\mathbb{Z}\left[\sqrt[3]{2}\right]$.

Example 3. The rational prime $p = 5$ has $\pi_1 = 1 + \sqrt[3]{2} - \sqrt[3]{4}$ and $\pi_2 = 1 + 2\sqrt[3]{2} - \sqrt[3]{4}$ as prime divisors; $N(\pi_1) = 5$ and $N(\pi_2) = 25$. The smallest prime p such that $p = m^2 + 27n^2$ is $p = 31$. This one has three non-associated prime divisors: $\pi_1 = -1 + 2\sqrt[3]{4}, \pi_2 = 3 - 3\sqrt[3]{2} + \sqrt[3]{4}, \pi_3 = 3 + \sqrt[3]{4}$.

5. Numerical Computations

The division algorithm and consequently the computations of greatest common divisors can be done by any computer algebra system. For the examples we used *Maple*. In *Maple* an element $a + b\sqrt[3]{2} + b\sqrt[3]{4}$ is entered as a triple (a, b, c). Product, quotient and norm are computed by:

```
> prod:=((a,b,c),(d,e,f))->
    array(1..3,[a*d+2*b*f+2*c*e,a*e+b*d+2*c*f,a*f+b*e+c*d]);
> conj:=(a,b,c)->array(1..3,[a^2-2*b*c,-a*b+2*c^2,-a*c+b^2]);
> n:=(a,b,c)->a^3+2*b^3+4*c^3-6*a*b*c;
> quot:=((a,b,c),(d,e,f))->
prod((a,b,c),(conj(d,e,f)[1]/n(d,e,f),conj(d,e,f)[2]/n(d,e,f),
conj(d,e,f)[3]/n(d,e,f)));
> N:=(a,b,c)->abs(n(a,b,c));
```

The division algorithm `div` returns the quotient and remainder if $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ is divided by $d + e\sqrt[3]{2} + f\sqrt[3]{4}$.

```
> div:=proc(a,b,c,d,e,f)local q,k,v,r;global R,w;
q:=quot((a,b,c),(d,e,f));
for k from 1 to 3 do v[k]:=floor(q[k]+0.5) end do;
if N(q[1]-v[1],q[2]-v[2],q[3]-v[3])<1 then w:=[v[1],v[2],v[3]] end if;
if N(q[1]-v[1],q[2]-v[2],q[3]-v[3])>=1 and q[1]-v[1]<=0 and q[2]-v[2]>=0
and q[3]-v[3]>=0 then w:=[v[1]-1,v[2],v[3]] end if;
if N(q[1]-v[1],q[2]-v[2],q[3]-v[3])>=1 and q[1]-v[1]>=0 and q[3]-v[3]>=0
and q[2]-v[2]<=0 then w:=[v[1],v[2]-1,v[3]] end if;
if N(q[1]-v[1],q[2]-v[2],q[3]-v[3])>=1 and q[1]-v[1]>=0 and q[2]-v[2]<=0
and q[3]-v[3]<=0 then w:=[v[1]+1,v[2],v[3]] end if;
if N(q[1]-v[1],q[2]-v[2],q[3]-v[3])>=1 and q[1]-v[1]<=0 and q[3]-v[3]<=0
and q[2]-v[2]>=0 then w:=[v[1],v[2]+1,v[3]] end if;
r:=matadd([a,b,c],-prod((w[1],w[2],w[3]),(d,e,f))):R:=[r[1],r[2],r[3]];
print(w,R); end proc:
```

And finally, using this division algorithm, the function `cgcd` computes the greatest common divisor of two elements in $\mathbb{Z}\left[\sqrt[3]{2}\right]$.

```
> cgcd:=proc(a,b,c,d,e,f) local g;
g[1]:=a:g[2]:=b:g[3]:=c:g[4]:=d:g[5]:=e:g[6]:=f:
div(g[1],g[2],g[3],g[4],g[5],g[6]):
while N(R[1],R[2],R[3])>0 do
g[1]:=g[4]:g[2]:=g[5]:g[3]:=g[6]:g[4]:=R[1]:g[5]:=R[2]:g[6]:=R[3]:
div(g[1],g[2],g[3],g[4],g[5],g[6]):  end do:
print([g[4],g[5],g[6]]); end proc:
```

References

[1] E.S. Barnes, H.P.F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms I, II, III, *Acta Math.*, **87** (1952), 259-323; ibid. **88** (1952), 279-316; ibid. **92** (1954), 199-234.

[2] Stefania Cavallar, Franz Lemmermeyer, The Euclidean algorithm in cubic number fields, *Number Theory* (1998), 123-146.

[3] B.N. Delone, D.K. Faddeev, The theory of irrationalities of the third degree, *Trans. Math. Monographs*, Am. Math, Soc., **10** (1964).

[4] H.J. Godwin, On Euclid's algorithm in some cubic fields with signature one, *Quart. J. Math. Oxford*, **18** (1967), 333-338.

[5] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York (1990).

[6] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York (1994).

[7] J.M. Pollard, Factoring with cubic integers, *The Development of the Number Field Sieve, Lecture Notes in Mathematics*, Volume **1554** (1993), 4-10.

[8] I.N. Stewart, D.O. Tall, *Algebraic Number Theory*, Chapman and Hall Ltd, London (1979).