

# Square Free Factorization for the integers and beyond

Kevin A. Broughan and Timothy E. Stokes

*University of Waikato, Hamilton, New Zealand*

E-mail: kab@waikato.ac.nz, stokes@waikato.ac.nz

Every positive integer has a unique decomposition as the product of powers of square free numbers which are a divisor chain. This generalizes to unique factorization domains (such as univariate polynomials over a field). However, it is shown that more general multiplicative structures exist for which unique square-free decomposition is possible.

**Keywords:** integer factorization, square free decomposition, polynomial factorization, Dedekind domain, semigroup.

**MSC2000:** 11A57, 13F15, 11Y05, 20M14, 68W05.

**Abbreviated Title:** Square Free Factorization

**Corresponding Author:**

Associate Professor Kevin A. Broughan,  
Department of Mathematics,  
University of Waikato,  
Private Bag 3105,  
Hamilton, New Zealand 2001,  
kab@waikato.ac.nz,  
fax 647-838-4666.

## 1. INTRODUCTION

The square free decomposition of a polynomial over a finite field is a very useful tool in computer algebra. It lies at the base of algorithms for complete polynomial factorization into irreducibles in that (a) it can be found easily using the derivative and greatest common divisor of polynomials, and (b) the commonly used Berlekamp algorithm, for factorization of a polynomial over a field with a prime number of elements, applies only to polynomials which are square free. For details see [7] or [8].

By contrast the square free decomposition of an integer is not so well known. In this paper integer upper and lower roots are used to derive a square free decomposition of any positive integer, which can be written in a unique manner.

These integer square roots are multiplicative. They have been used to study the class number of a quadratic field [1], the asymptotic order of the square free part of  $n!$  [2], generalized to  $k$ 'th roots [3] and used to derive consequences from weakened ABC conjectures [4].

If the standard factorization into primes of the positive integer  $n > 1$  is given by

$$n = \prod_{j=1}^m p_j^{\alpha_j}$$

then the lower integer square root is defined by

$$r(n) = \prod_{j=1}^m p_j^{\lfloor \frac{\alpha_j}{2} \rfloor}$$

and the upper integer square root by

$$R(n) = \prod_{j=1}^m p_j^{\lceil \frac{\alpha_j}{2} \rceil}.$$

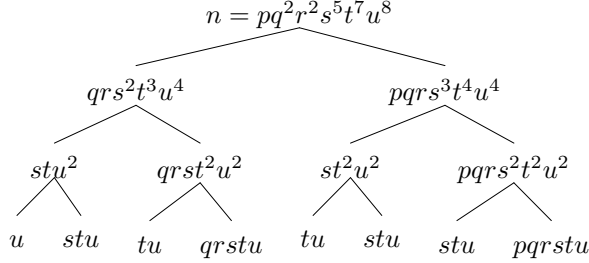
Since for all integers  $\alpha \geq 0$ ,

$$\alpha = \lfloor \frac{\alpha}{2} \rfloor + \lceil \frac{\alpha}{2} \rceil$$

it follows that  $n = r(n).R(n)$ . Continue with this process of decomposition, applying it to  $r(n)$  and  $R(n)$  until no new factors are found. For example, after two iterations the decomposition is

$$n = R(R(n)).r(R(n)).R(r(n)).r(r(n)).$$

This is illustrated with the example,  $n = pq^2r^2s^5t^7u^8$  where  $p, q, r, s, t, u$  are distinct primes. In the tree below, the two branches descending from a node  $m$  are  $r(m)$  on the left and  $R(m)$  on the right:



## 2. SQUARE FREE FACTORS OF A RATIONAL INTEGER

Let  $n \in \mathbb{N}$  and let

$$n = \prod_{j=1}^m a_j^{\alpha_j}$$

be the factorization of  $n$  produced by iterating the decomposition  $n = R(n).r(n)$  until no new factors are found and then collecting like factors.

LEMMA 2.1. *Each  $a_i$  is square free.*

*Proof.* If  $n$  is not square free then  $n = a^2b$  with  $a \neq 1$  and  $b$  square free and  $n = r(n).R(n) = a.(ab)$  is a non trivial factorization. If  $n$  is square free then  $n = 1.N(n)$  so no new factors are formed. The result follows by induction on iterations. ■

LEMMA 2.2. *If  $p, q \in \mathbb{P}$  are such that  $\text{ord}_p(n) = \text{ord}_q(n)$  then  $p \mid a_i$  if and only if  $q \mid a_i$  for all  $i$ .*

*Proof.* If  $\text{ord}_p(n) = \text{ord}_q(n)$  then  $p \mid R(n)$  if and only if  $q \mid R(n)$  and  $p \mid r(n)$  if and only if  $q \mid r(n)$  and the result follows by induction on iterations. ■

LEMMA 2.3. *If the standard prime factorization of  $n$  is written*

$$n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$$

*with  $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_l$  then each  $a_i$  is the product of an initial segment of the primes, i.e. for all  $i$  there is a  $j_i$  such that  $a_i = p_1 \cdots p_{j_i}$ .*

*Proof.* In the decomposition  $n \rightarrow (r(n), R(n))$ , all primes which occur in  $n$  are also in  $R(n)$ . Exactly those primes in  $n$  which occur to the power 1 are lost in  $r(n)$ . These occur at the bottom of the given ordering of prime factors. So, again by induction, the primes which are left in  $a_i$  form an initial segment of the primes which occur in  $n$ . ■

LEMMA 2.4. *There exists an ordering for the  $(a_i)$  such that  $a_1 \mid a_2 \mid \cdots \mid a_m$ .*

*Proof.* Since each  $a_i$  is square free and its factors form an initial segment of the original primes in  $n$ , when written in order of decreasing powers, the divisibility relationships follow. ■

LEMMA 2.5. *If the highest power of a prime occurring in the standard factorization of  $n$  is  $\beta \geq 2$ , then the process terminates before  $\log(\beta)/\log(4/3)$  iterations.*

*Proof.* At each iteration the highest power of a prime, say  $\gamma$ , decreases to either  $\gamma/2$  if  $\gamma$  is even, or  $(\gamma + 1)/2$  if  $\gamma$  is odd. In either case one step reduces the power to less than or equal to  $3\gamma/4$  for all  $\gamma \geq 2$ . ■

### 3. UNIQUE SQUARE FREE FACTORIZATION

THEOREM 3.1. *If  $n \in \mathbb{N}$  has a factorization*

$$n = \prod_{j=1}^m a_j^{\alpha_j}$$

*with the  $(a_j)$  distinct and square free and  $a_1 \mid a_2 \mid \cdots \mid a_m$  then, with these properties, this factorization is uniquely determined.*

*Proof.* We will construct a proof using induction on  $m$ , the number of distinct square free factors. So let

$$n = \prod_{j=1}^m a_j^{\alpha_j} = \prod_{i=1}^l b_i^{\beta_i}$$

where the  $(\beta_i)$  are distinct and square free and  $b_1 \mid b_2 \mid \cdots \mid b_l$ .

If  $l = 1$  then every prime which divides  $n$  does so to the power  $\beta_1$ . By Lemma 2,  $m = 1$  so  $a_1^{\alpha_1} = b_1^{\beta_1}$ . Since  $a_1$  and  $b_1$  are square free we must have  $a_1 = b_1$  and  $\alpha_1 = \beta_1$ . Hence if there are two representations and one has one power the representations are the same.

Now assume the representation is unique for us to  $m$  terms for some  $m \geq 1$ , i.e. if

$$n = \prod_{j=1}^m a_j^{\alpha_j} = \prod_{i=1}^l b_i^{\beta_i}$$

for some  $l \in \mathbb{N}$  then  $l = m$ ,  $a_i = b_i$ ,  $\alpha_i = \beta_i$  for  $1 \leq i \leq m$ . Consider

$$n = \prod_{j=1}^{m+1} a_j^{\alpha_j} = \prod_{i=1}^l b_i^{\beta_i}.$$

If  $l \leq m$  we are done (by the inductive hypothesis exchanging the roles of  $a_j$  and  $b_i$ ), so assume  $l \geq m + 1$ .

Then  $a_{m+1} \mid n$  and is square free so  $a_{m+1} \mid \beta_l$  by Lemma 4. Similarly  $b_l \mid a_{m+1}$  so  $a_{m+1} = b_l$ .

Now consider a prime  $p$  which divides  $n$  so that  $\text{ord}_p(n)$  is a maximum. Since  $p \mid a_1$  and  $a_1 \mid \cdots \mid a_{m+1}$  we have

$$p^{\alpha_1 + \cdots + \alpha_{m+1}} \parallel b_1^{\beta_1} \cdots b_l^{\beta_l}$$

so  $\alpha_1 + \cdots + \alpha_{m+1} = \beta_1 + \cdots + \beta_l$ . Now consider a prime  $q$  which divides  $n$  to the next most maximum power e.t.c. This leads to a set of equations in the powers  $(\alpha_j), (\beta_i)$  which may be "solved" in reverse order to obtain the given implications:

$$\begin{aligned} \alpha_1 + \cdots + \alpha_{m+1} &= \beta_1 + \cdots + \beta_l \implies \alpha_1 = \beta_1 \\ \alpha_2 + \cdots + \alpha_{m+1} &= \beta_2 + \cdots + \beta_l \implies \alpha_2 = \beta_2 \\ &\dots = \dots \\ &\dots = \dots \implies \alpha_m = \beta_m \\ \alpha_{m+1} &= \beta_{m+1} + \cdots + \beta_l. \end{aligned}$$

Therefore we can write

$$a_1^{\alpha_1} \cdots a_m^{\alpha_m} a_{m+1}^{\alpha_{m+1}} = b_1^{\alpha_1} \cdots b_m^{\alpha_m} b_{m+1}^{\beta_{m+1}} \cdots b_l^{\beta_l}.$$

Let the prime  $p \mid a_{m+1}$  and  $p \nmid a_m$ . Then

$$\begin{aligned} \text{ord}_p(a_{m+1}^{\alpha_{m+1}}) &= \alpha_{m+1} = \beta_{m+1} + \cdots + \beta_l \\ &= \text{ord}_q(b_{m+1}^{\beta_{m+1}} \cdots b_l^{\beta_l}) \end{aligned}$$

where the prime  $q \nmid b_m$ .

Hence

$$a_{m+1}^{\alpha_{m+1}} = b_{m+1}^{\beta_{m+1}} \cdots b_l^{\beta_l}$$

and the result follows from the step  $m = 1$ .  $\blacksquare$

#### 4. POSSIBLE GENERALIZATIONS

First note that the previous arguments can easily be extended to general unique factorization domains (UFD's), including the ring of univariate polynomials over a field, where the idea of square-free decomposition has had most attention so far. For algebraic number rings and fields, important examples need not be UFD's, e.g. if  $R = \mathbb{Z}[\sqrt{d}]$ , where  $d < 0$  is a square free integer [5, 10, 11], unique factorization fails unless

$$d \in \mathbf{H} = \{-1, -2, -7, -11, -19, -43, -67, -163\},$$

the so-called Heegner numbers [12, 13].

More generally than these "quadratic fields" are rings of integers of finite algebraic extensions of  $\mathbb{Q}$  which are examples of Dedekind domains: these are commutative rings which are integral domains, Noetherian (no infinite ascending chains of ideals), integrally closed, and every non-zero prime ideal is maximal [6]. In the setting of Dedekind domains, unique factorization can be rescued, but at the level of ideals and not individual ring elements. Every ideal  $I$  can be expressed uniquely as the product of integer powers of prime ideals:

$$I = P_1^{\alpha_1} \cdots P_m^{\alpha_m},$$

where the (associative) multiplication of ideals  $A, B$  is defined by

$$A.B = \left\{ \sum_{i=1}^n r_i a_i b_i : r_i \in R, a_i \in A, b_i \in B \right\}.$$

Square-freeness for ideals could be defined using the radical operation on ideals defined as follows. If  $I$  is any ideal then

$$\text{rad } I = \{x \in R : x^n \in I \text{ for some } n \in \mathbb{N}\}.$$

An ideal  $I$  is said to be radical if  $\text{rad } I = I$ . In the ring  $\mathbb{Z}$ , an ideal  $I = (m)$  is radical if and only if  $m$  is square free. Hence the analogy with factorization of ideals leads to a decomposition

$$I = A_1^{\alpha_1} \cdots A_m^{\alpha_m},$$

where each  $A_i$  is radical and  $A_1 \mid A_2 \mid \cdots \mid A_m$  and where division of ideals, in this Dedekind domain setting, can be defined via inclusion:  $A \mid B$  if and only if  $B \subset A$ . Note that in Dedekind domains an ideal is radical if and only if it is the intersection of a finite number of prime ideals.

The question of interest is when and how a translation back to elements of the number field may be made. For example if every radical ideal is principal we can produce a unique square free decomposition of any element of  $\mathbb{Z}[\sqrt{d}]$ , even when unique factorization does not hold. So, more precisely, are there any values of  $d < 0$ , in addition to those in  $\mathbf{H}$ , in which every prime ideal is principal, and thus for which a unique square free decomposition may be derived?

This quest is too hopeful: exploration of the first two values of  $d$  for which unique factorization fails,  $d = -5$  and  $d = -6$ , delivers a negative result:

$$\begin{aligned} \mathbb{Z}[\sqrt{-5}] &: -2 + 8i\sqrt{5} = 2(2 + i\sqrt{5})^2 = (-2 - i\sqrt{5})(-1 + i\sqrt{5})^2 \\ \mathbb{Z}[\sqrt{-6}] &: 12 = (-2)(i\sqrt{6})^2 = 3 \cdot 2^2. \end{aligned}$$

where  $-2 - i\sqrt{5}$  in  $\mathbb{Z}[\sqrt{-5}]$  and  $-2$  in  $\mathbb{Z}[\sqrt{-6}]$  are square free. (We found these examples by enumeration: we computed the numbers, the squares, the products of numbers and squares and then took complements to find the square free numbers up to a given value of the norm  $N[m + \sqrt{d}n] = m^2 - dn^2$ . We then examined the products of squares with square free numbers, up to the given value of the norm, to find duplicates.)

A more individual ring element oriented approach to establishing when unique square free decompositions exist would be the following: Let  $R$  be an integral domain with 1. We say  $x \in R$  is **square free** if  $y^2 \mid x$  implies  $y$  is a unit in  $R$ . Then if  $x$  is square free so is every divisor of  $x$ . If  $x$  is prime or irreducible then it is square free. In a number field, if the norm of  $x$  (the product of the conjugates of  $x$ ) is square free then so is  $x$ .

If  $a$  and  $b$  are in  $R$  we say they are a **divisor independent pair** if their only common divisor is an associate of 1. Then if  $a, b$  are divisor independent, so is every pair of divisors of  $a, b$  respectively.

We say  $R$  satisfies condition (A) if whenever  $a \mid x$  and  $b \mid x$  and  $a, b$  are divisor independent, then  $ab \mid x$ . We say  $R$  satisfies condition (B) if whenever  $a, b$  are divisor independent so is  $a^2, b^2$ . We say  $R$  satisfies condition (M) if there are no infinite ascending chains of principal ideals. Finally we say  $R$  satisfies  $(\rho)$  if every irreducible element is prime.

Any unique factorization domain satisfies (A), (B) and (M). If  $d < 0$  then  $\mathbb{Z}[\sqrt{d}]$  satisfies (M). Both (A) and (B) fail in  $\mathbb{Z}[\sqrt{-6}]$ .

If  $R$  satisfies (A), (B) and (M), a unique square free decomposition may be derived as follows:

Let  $x \in R$  be any element and order the proper divisors of  $x$  by division, i.e.  $a < b$  if  $a|b$ . Then if  $R$  satisfies (C) and  $y^2$  is a maximal squared divisor, then  $z = x/y^2$  is square free, leading to the square free decomposition  $x = y^2 \cdot z$ . This process can be iterated, applying it to  $y$  e.t.c until we are left with an element which is itself square free, so the process stops. The elements of the decomposition can then be rearranged to be consistent with the form given in Theorem 1. So a square free decomposition exists, for example, in imaginary quadratic fields.

As for uniqueness, here we use (A) and (B): If  $z = a^2b = x^2y$  with  $b, y$  square free and not units, then, through eliminating common factors, we can assume that  $a, x$  and  $b, y$  are divisor independent. But then  $x^2 | a^2b$  and  $a^2 | a^2b$  and  $a^2, x^2$  are, by (B), divisor independent, so therefore, by (A),  $x^2 \cdot a^2 | a^2b$  so  $x^2 | b$ . Since  $b$  is square free this means  $x$  is a unit, so therefore  $(a/x)^2b = y$  so  $a/x$  is a unit also. Hence  $a \sim x$  and  $b \sim y$  and the square free decomposition is unique.

So (A), (B) and (M) are natural conditions which give unique square free decompositions. However (A) is already very strong, since  $R$  is a unique factorization domain if and only if it satisfies (M) and  $(\rho)$ , and, as will be shown, (A) implies  $(\rho)$ :

**THEOREM 4.1.** *If the integral domain  $R$  satisfies (A) then every irreducible element is prime.*

*Proof.* Let  $x$  be irreducible and  $x | ab$  in  $R$ . If  $x$  and  $a$  have a non-unit common divisor  $d$  then it must be an associate of  $x$ , in which case  $x | a$ . If  $x \nmid a$  then  $(x, a) = 1$ . But  $x | ab$  and  $a | ab$ , so by (A),  $xa | ab$ , and therefore  $x | b$ . Thus  $x$  is prime. ■

It follows that in the presence of (M), (A) and  $(\rho)$  are equivalent. (In one sense, (A) is more natural than  $(\rho)$  since it makes no reference to prime or irreducible elements in the ring.) The central issue remains: find natural conditions, demonstrably weaker than unique factorization, which give unique square free decompositions in integral domains.

One can fruitfully broaden this question by first noting that the arguments of the previous section really only depend on the structure of the multiplicative semigroup of positive integers. Thus the element  $2^3 \times 3 \times 7^5 \times 11^3$  can be represented as  $x = (3, 1, 0, 5, 3, 0, 0, \dots)$  in the countable direct sum of copies of the naturals with zero. Multiplication of integers then corresponds to addition of elements in the direct sum, and upper and lower square roots can easily be expressed also. In the example, the upper and lower square roots of  $x$  are

$$R(x) = (2, 1, 0, 3, 2, 0, 0, \dots) \text{ and } r(x) = (1, 0, 0, 2, 1, 0, 0, \dots).$$

Note that square-free products are just direct sum elements all of whose non-zero entries are 1. It is then not hard to show that the square-free decomposition may be obtained from the direct sum representation as follows.

- Let  $y_1 = C(x)$  be the direct sum element which has 1 where  $x$  is non-zero and 0 otherwise.
- Let  $\alpha_1$  be the smallest non-zero entry in  $x$ , and let  $x_1 = x - \alpha_1 y_1$ .
- Proceeding recursively, for  $i \geq 1$ , let  $y_{i+1} = C(x_i)$ , let  $\alpha_{i+1}$  be the smallest non-zero entry in  $x_i$ , and let  $x_{i+1} = x_i - \alpha_{i+1} y_{i+1}$ .
- Stop when  $x_n$  has only zero entries.

It then follows that  $x = \sum_{i=1}^n \alpha_i y_i$  is the unique square-free decomposition of  $x$  for which  $y_n \mid y_{n-1} \mid \cdots \mid y_1$ .

Similar direct sum representations apply in any UFD - each entry corresponds to a particular prime element (working modulo associates), and indeed all the earlier arguments as well as those just given apply to general UFD's too, with little modification. Can the arguments be extended beyond UFD's in some way?

Given the multiplicative nature of the problem, one could broaden this question: are there generalisations of direct sums of the non-negative integers under addition for which unique square-free decomposition exists? The problem then becomes one of (cancellative) commutative semigroup theory, where one can define notions such as "square-free", "irreducible" and "prime" in the expected ways. The answer to this generalised question turns out to be "yes".

Let  $A$  be the subsemigroup of the countable Cartesian product of copies of the non-negative integers for which all but finitely many entries are some fixed integer - the "ultimately constant" sequences. This semigroup evidently contains the countable direct sum, where the constant is always zero. Given such a sequence, exactly the same method of obtaining unique square-free decompositions as just given above applies: the process of obtaining the decomposition terminates and has the desired form. Now, irreducibles in  $A$  are elements having 1 in one entry and zero elsewhere, just as before, but such elements are not "prime": for example the element  $(1, 1, 1, \dots)$  cannot be expressed as a *finite* sum of such irreducible elements. However, it is unlikely that any ring can be constructed which has  $A$  as its multiplicative semigroup.

An example along similar lines for which unique square-free decompositions exist, but for which there is no computable algorithm to find them, is obtained by replacing "ultimately constant" by "bounded" - the recursive definition of the  $y_i$  and  $\alpha_i$  still makes sense, and there will be only finitely many of them in a representation, but the  $y_i$  and  $\alpha_i$  are not computable,

since the representation of  $x$  cannot be given using finitely many bits of information.

### ACKNOWLEDGMENT

The authors acknowledges helpful conversations with Ian Hawthorn and Pat Gallagher, and the support given by the University of Waikato and Columbia University.

### REFERENCES

1. Broughan, K. A.: Restricted Divisor Sums. *Acta Arithmetica* **101**, 105-114(2002)
2. Broughan, K. A.: Asymptotic Order of the square free part of  $n!$ . *Integers: Electronic Journal of Combinatorial Number Theory* **2,A10**, 1-6 (2002)
3. Broughan, K. A.: Relations between the conductor and integer  $k$ 'th roots. *International Journal of Pure and Applied Mathematics* **5**, 253-275 (2003)
4. Broughan, K. A.: Relaxations of the ABC conjecture using integer  $k$ 'th roots, (preprint).
5. Cohn, H., *A second course in number theory*, Wiley, 1962
6. Dummit, D. S. and Foote, R. M., *Abstract Algebra*, Second Edition, Prentice-Hall, 1999
7. Davenport, J. H. Siret, Y. and Tournier, E., *Computer Algebra*, Academic Press, 1988
8. von zur Gathen, J. and Gerhard, J., *Modern Computer Algebra*, Cambridge, 1999
9. Geddes, K.O., Czapor, S.R. and G. Labahn, G., *Algorithms for Computer Algebra*, Kluwer Academic Publishers, 1992
10. Goldman, J.O., *The Queen of Mathematics*, A. K. Peters, 1996
11. Hardy, G.H. and Wright, E.M., *An introduction to the theory of numbers*, Fifth Edition, Oxford, 1979
12. Heegner, K.: Diophantische Analysis and Modulfunktionen. *Math. Z.* **56**, 227-253 (1952)
13. Stark, H.: A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.* **14**, 1-27 (1967)