ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 32, Number 4, Winter 2002

ON UNIT SUM NUMBERS OF RATIONAL GROUPS

B. GOLDSMITH, C. MEEHAN AND S.L. WALLUTIS

ABSTRACT. The unit sum numbers of rational groups are investigated: the importance of the prime 2 being an automorphism of the rational group is discussed and other results are achieved by considering the number and distribution of rational primes which are, or are not, automorphisms of the group. Proof is given of the existence of rational groups with unit sum numbers greater than 2 but of finite value.

1. Introduction. The relationship between the groups of units of a unital associative ring and the ring itself has been studied in various forms over a long number of years. Prompted by a question of Fuchs [**6**], there has been special interest in the situation in which the ring is the full endomorphism ring of an abelian group, or more generally a module, and the group of units is then the corresponding automorphism group. Recall the definitions from [**10**]: an associative ring $\mathbf{R}$ is said to have the *n-sum property* (for a positive integer n), if every element of $\mathbf{R}$ can be written as the sum of exactly n units of $\mathbf{R}$. Clearly, if this property holds for an integer n, then it also holds for any integer $k > n$, and so we can make the following definition of the unit sum number of a ring $\mathbf{R}$: $\mathrm{usn}\,(\mathbf{R}) := \min\{n \mid \mathbf{R} \text{ has the } n\text{-sum property}\}$. If there is an element of $\mathbf{R}$ which is not a sum of units, we set the unit sum number to be ∞, while if every element of $\mathbf{R}$ is a sum of units but $\mathbf{R}$ does not have the n-sum property for any n, we set $\mathrm{usn}\,(\mathbf{R}) = \omega$. The unit sum number of an abelian group or module is defined to be equal to that of its endomorphism ring. There is a considerable body of literature on this topic, often without using the terminology above. The principal works include [**2**], [**5**], [**9**]–[**11**], [**14**], [**16**]–[**18**].

A notable feature of all previous works is that the only finite values determined for a unit sum number have been 1 and 2, the former corresponding to the trivial situation. The focus of the current work is the problem of calculating unit sum numbers of rational groups, i.e.,

1991 AMS *Mathematics Subject Classification.* Primary 20K30, 20K15.
Received by the editors on July 28, 2001, and in revised form on October 8, 2001.

subgroups of the additive group of rational numbers $\mathbf{Q}$. As is well known, the endomorphism ring of a rational group is a subring of the rationals $\mathbf{Q}$, i.e., we actually investigate these rings. For convenience, we shall refer to such rings as *rational rings*. Note that all rational rings except $\mathbf{Q}$ itself can also be realized as endomorphism rings of arbitrarily large groups (see [**3**], [**4**]). Although we have a very concrete description of such groups in terms of types (see [**6**, p. 107]), it is not a simple problem to calculate the unit sum numbers: difficult number-theoretic issues arise and, as we shall indicate in Section 4, a relationship exists between our problem and some known approaches to additive number theory. Our principal result is the rather surprising one that a ring with finite unit sum number exists which is strictly greater than two.

Our terminology is standard and may be found in Fuchs [**6**], [**7**]; an exception is that we write maps on the right and we denote the set of rational primes by Π. Concepts from number theory may be found in Prachar [**15**] and from additive number theory in Nathanson [**13**]; in particular, we shall have need of the function $\pi(x)$ defined for a real number x as the number of rational primes not exceeding x and also the function $\pi(x, k, l)$ defined, for a real number x and positive integers k, l with $(k, l) = 1$ as the number of rational primes congruent to l mod k and not exceeding x. We also adopt the standard practice, where necessary, of distinguishing a ring from a module by using boldface characters for the former.

2. General considerations. As mentioned in the introduction, our consideration of unit sum numbers of rational groups reduces to the study of rational rings. The following two results reflect the importance of the prime number 2 in determining the unit sum numbers of rational groups and rings.

Proposition 2.1. *Let* $\mathbf{R}$ *be a rational ring. If* 2 *is not a unit of* $\mathbf{R}$, *then* $\operatorname{usn}(\mathbf{R}) = \omega$.

Proof. Consider an element a/b of $\mathbf{R}$ where a, b are positive integers. If b is even, then $(a/b)(b/2) = (a/2)$ is an element of $\mathbf{R}$. Therefore, a must be even or else $(a-1)/2 \in \mathbf{Z}$ in which case $(a/2) - [(a-1)/2] = (1/2)$ must be an element of $\mathbf{R}$, contradicting 2 not being a unit of $\mathbf{R}$.

Therefore, if a/b is a unit of $\mathbf{R}$, expressed in lowest form, then both a and b must be odd.

Let n be any even positive integer. Consider any sum of n units of $\mathbf{R}$,

$$\frac{a_1}{b_1}+\frac{a_2}{b_2}+\cdots+\frac{a_n}{b_n}=\frac{a_1b_2\dots b_n+a_2b_1b_3\dots b_n+\cdots+a_nb_1\dots b_{n-1}}{b_1\dots b_n},$$

where a_i/b_i is a unit of $\mathbf{R}$ expressed in lowest form for each $i=1,2,\dots,n$. Observe that the denominator is a product of odd numbers and therefore odd and the numerator is an even sum of odd number products and therefore even. A sum of n units can never be a unit in this case. Therefore $\mathbf{R}$ does not have the n-sum property for any even integer n. We know, however, that for any positive n a ring which has the n-sum property must also have the $(n+1)$-sum property. It follows that $\mathbf{R}$ cannot have the n-sum property for any positive integer n. Every element of $\mathbf{R}$ is a sum of units so we conclude that $\operatorname{usn}(\mathbf{R})=\omega$.

Proposition 2.2. *The rational ring* $\mathbf{Q}^{(2)}$ *of type* $(\infty,0,0,\dots)$ *has unit sum number* ω.

Proof. We prove that, for each positive integer n, there is an integer, namely $1+2^2+\cdots+2^n$, which cannot be expressed as a sum of n units of $\mathbf{Q}^{(2)}$. Now in $\mathbf{Q}^{(2)}$ each unit is of the form $\pm 2^a$ where a is an integer.

The proof is by induction on $n\in\mathbf{N}$ where the induction statement is

$$(*)\qquad 1+2^2+\cdots+2^{2n}\neq\sum_{i=1}^{n}\pm 2a^{a_i}\quad\text{for whatever } a_i\in\mathbf{Z}.$$

The statement is true for $n=1$ since $1+2^{2(1)}=5$ and 5 is not a unit. We assume the statement is true for all positive integers $n<m$. Now, seeking a contradiction, assume

$$(1)\qquad 1+2^2+\cdots+2^{2m}=\sum_{i=1}^{m}\pm 2^{a_i}$$

for some fixed set of integers $a_1,\dots,a_m$. The lefthand side of this equation is odd and hence the set $\{i\mid a_i<2\}$ is nonempty. By

renumbering, we can arrange that there is an $l \in \mathbf{N}$, $l \leq m$, such that $a_i < 2$ for $i = 1, \ldots, l$ and $a_i \geq 2$ for $i = l+1, \ldots, m$. Hence we can rewrite equation (1) as

$$2^2 + \cdots + 2^{2m} = \left(\sum_{i=1}^{l} \pm 2^{a_i} \right) - 1 + \sum_{i=l+1}^{m} \pm 2^{a_i}. \tag{2}$$

We claim that the term $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1$ can be written as a sum of less than l units in $\mathbf{Q}^{(2)}$ unless it is zero. Observe from the equation that 4 divides $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1$. So, writing $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1 = 4l'$ for some $l' \in \mathbf{Z}$, we note that this expresses $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1$ as a sum of $|l'|$ units for $l' \neq 0$.

It remains to show that $|l'| < 1$ for $l' \neq 0$.

Since $2^{a_i} \leq 2$ for all $a_i < 2$, it is clear that

$$\left| \left(\sum_{i=1}^{l} \pm 2^{a_i} \right) - 1 \right| = |4l'| \leq 2l + 1.$$

Therefore we have $|2l'| + 1 < 2l + 1$ which gives us $|l'| < l$ as $l' \neq 0$. The claim is proved.

Returning to equation (2), since $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1$ is either zero or can be expressed as a sum of less than l units, then $2^2 + \cdots + 2^{2m}$ can be expressed as a sum of less than m units. Thus we may write

$$2^2 + \cdots + 2^{2m} = \sum_{j=1}^{m'} \pm 2^{b_j} \quad \text{for some } m' < m, b_j \in \mathbf{Z}.$$

Dividing this equation by 4, we get

$$1 + \cdots + 2^{2(m-1)} = \sum_{j=1}^{m'} \pm 2^{b_j - 2}.$$

This contradicts the induction statement $(*)$ for $n = m - 1$ since any sum of $m' \leq m-1$ units can easily be expressed as a sum of $m'+1, m'+2, \ldots, m-1$ units by putting $\sum_{i=1}^{m'} u_i = \sum_{i=1}^{m'-1} u_i + (1/2)u_{m'} + (1/2)u_{m'}$

where each u_i is a unit, and repeating. Hence the assumption (1) is false and the proof now follows by induction. Therefore, $\operatorname{usn}(\mathbf{Q}^{(2)}) = \omega$.

The next two lemmas enable us to make some simplifications in our approach.

Lemma 2.3. *Let* $\mathbf{R}$ *be a rational ring. If* 2 *is a unit of* $\mathbf{R}$*, then* $\mathbf{R}$ *has the* n*-sum property if and only if every positive integer is a sum of exactly* n *units of* $\mathbf{R}$.

Proof. Clearly, if $\mathbf{R}$ has the n-sum property for some positive integer n, then every positive integer is a sum of n units of $\mathbf{R}$.

Conversely, suppose every positive integer is expressible as a sum of n units of $\mathbf{R}$. Then every negative integer must also be expressible as a sum of n units of $\mathbf{R}$ and, since

$$0 = 1 - \sum_{i=1}^{n-2} \frac{1}{2^i} - \frac{1}{2^{n-2}},$$

all integers are sums of n units.

Consider an arbitrary noninteger element of $\mathbf{R}$, a/b, expressed in lowest form.

If $a = 1$, then (a/b) is a unit. Since products of units are units and 1 is a sum of n units, then $(a/b)(1)$ is also.

If $b = 1$, then $a/b = a$, an integer, and so is a sum of n units.

In any remaining case a and b must be relatively prime so integers k, l exist such that $ka + lb = 1$. Now $(k(a/b) + l)$ is an element of $\mathbf{R}$ and $(k(a/b) + l)(b) = 1$. Therefore, b is a unit of $\mathbf{R}$ and so also is $1/b$. Since a, as an integer, is a sum of n units, then $1/b(a)$ is also.

Lemma 2.4. *Let* $\mathbf{R}_1, \mathbf{R}_2$ *be rational rings with* $\mathbf{R}_1 \leq \mathbf{R}_2$*, then* $\operatorname{usn}(\mathbf{R}_1) \geq \operatorname{usn}(\mathbf{R}_2)$.

Proof. There is no loss in generality in assuming 2 is a unit in $\mathbf{R}_1$ for otherwise $\operatorname{usn}(\mathbf{R}_1) = \omega$. Since $\mathbf{R}_1 \leq \mathbf{R}_2$ every unit of $\mathbf{R}_1$ is a unit of $\mathbf{R}_2$. So if a positive integer z is a sum of n units in $\mathbf{R}_1$, then

the same is true for z as an element of $\mathbf{R}_2$. Therefore, by Lemma 2.3, $\operatorname{usn}(\mathbf{R}_2) \leq \operatorname{usn}(\mathbf{R}_1)$.

3. Unit sum numbers for various rational rings. Given the description of the rational ring $\mathbf{R}$ in terms of the type, it is natural to consider the set $X_R := \{p \in \Pi \mid (1/p) \notin \mathbf{R}\}$; clearly X_R is the set of primes which are not units of $\mathbf{R}$.

Theorem 3.1. *Let* $\mathbf{R}$ *be a rational ring where* 2 *is a unit of* $\mathbf{R}$*. If* X_R *is finite, then* $usn(\mathbf{R}) = 2$.

Proof. Let $X_R = \{q_i \mid i = 1, \ldots, k\}$ where $k = |X_R|$. By Lemma 2.3, we need only prove all positive integers are sums of two units of $\mathbf{R}$. Clearly, as 2 is a unit of $\mathbf{R}$ then every unit of $\mathbf{R}$ is a sum of two units. Now, by definition of X_R, we know that for all $p \in \Pi \setminus X_R$, p is a unit of $\mathbf{R}$ and so any products of primes not in X_R are units of $\mathbf{R}$. Let $z = (\prod_{i=1,\ldots,k} q_i^{m_i})(\prod_{p_j \in \Pi \setminus X_R} p_j^{n_j})$ with $m_i, n_j \in \omega$ an arbitrary positive integer which is not a unit in $\mathbf{R}$, i.e., some $q_i \in X_R$ divides z.

Since $(\prod_{p_j \in \Pi \setminus X_R} p_j^{n_j})$ is a unit we need only show that $z' = (\prod_{i=1,\ldots,k} q_i^{m_i})$ is a sum of two units of $\mathbf{R}$. If every q_i in X_R divides z', then $(z' - 1)$ is relatively prime to all $q_i \in X_R$ and therefore a unit, in which case $z' = (z' - 1) + 1$ is a sum of two units for z'.

If some q_i in X_R does not divide z', then $(z' \pm \prod_{q_i \nmid z'} q_i)$ is a unit since no prime in X_R can divide it. In this way, $z' = (z' + \prod_{q_i \nmid z'} q_i)/2 + (z' - \prod_{q_i \nmid z'} q_i)/2$ expresses z' as a sum of two units and the result follows.

Theorem 3.1 can be extended to show that there are many rational rings having a countably infinite set of primes which are not units, yet with unit sum number of 2. The following result is similar to that of Opdenhövel [**14**, IV, Theorem 1.20], though it is arrived at in a completely different way. We will illustrate the proposition with an example after the proof. Recall that $\pi(x)$ is defined for a real number x as the number of rational primes not exceeding x.

Proposition 3.2. *Let* $\mathbf{R}$ *be a rational ring where* 2 *is a unit of* $\mathbf{R}$. *Moreover, assume that, for any* $x \in \mathbf{N}$ *with* $(x,p) = 1$ *for all* $p \in \Pi \setminus X_R$ *there is some prime* $q > x$ *so that* $q' \notin X_R$ *for all* $q' \in \Pi$ *with* $q \leq q' < q^{\pi(q)}$. *Then* $\operatorname{usn}(\mathbf{R}) = 2$.

Proof. By Lemma 2.3 it is only necessary to show that every positive integer is a sum of two units of $\mathbf{R}$. Since 2 is a unit of $\mathbf{R}$, every unit is a sum of two units. Each $p \in \Pi \setminus X_R$ is a unit of $\mathbf{R}$ and, since products of units are units, it is sufficient to show that products of elements of $X_R = \{q_i \mid i \in I\}$ are sums of two units of $\mathbf{R}$.

Let $x \in \mathbf{N}$ be such that $(x,p) = 1$ for all $p \in \Pi \setminus X_R$, i.e., x is a product of primes in X_R and $x \geq 3$. By assumption, there is some $q \in \Pi$ with $x < q$ so that $q' \notin X_R$ for all $q' \in \Pi$ with $q \leq q' < q^{\pi(q)}$. Then we claim that the following expresses x as a sum of two primes:

$$x = \frac{1}{2}\Big(x + \prod_{\substack{q_i \nmid x \\ q_i < q}} q_i\Big) + \frac{1}{2}\Big(x - \prod_{\substack{q_i \nmid x \\ q_i < q}} q_i\Big).$$

To prove this claim we need to show that $(x + \prod_{q_i \nmid x; q_i < q} q_i)$ is a unit of $\mathbf{R}$. Let $p \in \Pi$ be such that p divides $(x + \prod_{q_i \nmid x; q_i < q} q_i)$. We show that $p \notin X_R$.

If $p < q$, since all primes in X_R less than q are accounted for by the prime factors of x and $(\prod_{q_i \nmid x; q_i < q} q_i)$, then p cannot divide both x and $\prod_{q_i \nmid x; q_i < q} q_i$ so $p \notin X_R$.

If $q \leq p < q^{\pi(q)}$, then $p \notin X_R$ by the condition that $q' \notin X_R$ for all $q' \in \Pi$ with $q \leq q' < q^{\pi(q)}$.

Now we consider $q^{\pi(q)} \leq p$. Note that, by assumption, $x < q$ and $q > 3$ and so $q^{\pi(q)} > q^{\pi(q)-1} + q$. Also notice that $|\{i \in I; q_i < q\}| < \pi(q) - 1$, since $2 \notin X_R$ and thus $(\prod_{q_i \nmid x; q_i < q} q_i) < (\prod_{q_i < q} q_i) < q^{\pi(q)-1}$. Therefore, $|(x + \prod_{q_i \nmid x; q_i < q} q_i)| < q + q^{\pi(q)-1} < q^{\pi(q)}$. So $p \geq q^{\pi(q)}$ cannot divide $(x + \prod_{q_i \nmid x; q_i < q} q_i)$ since it is too big. Therefore the integer $(x + \prod_{q_i \nmid x; q_i < q} q_i)$ must be a product of primes not contained in X_R and therefore a unit of $\mathbf{R}$. By a similar argument $(x - \prod_{q_i \nmid x; q_i < z} q_i)$ is also a unit of $\mathbf{R}$.

Example 3.3. Denote by $\tau^1[n]$, $n \in \mathbf{N}$, the index of the least prime greater than $p_n^{\pi(p_n)}$ (i.e., $p_{\tau^1[n]}$ is the least prime greater than $p_n^{\pi(p_n)}$) and set $\tau^1[\tau^{(m-1)}[n]] = \tau^m[n]$ for all integers $m > 1$.

Let $\mathbf{R}$ be the subring of $\mathbf{Q}$ with type $(\mathbf{R}) = (k_{p_i})$ where

$$k_{p_i} = \begin{cases} \infty & \text{for } i = 1, \\ 0 & \text{for } 1 < i \leq \tau^1[2] \\ \infty & \text{for } \tau^1[2] < i \leq \tau^2[2] \\ \dots & \dots \\ 0 & \text{for } \tau^j[2] < i \leq \tau^{j+1}[2],\ j(>1) \text{ even} \\ \infty & \text{for } \tau^j[2] < i \leq \tau^{j+1}[2],\ j(>1) \text{ odd.} \end{cases}$$

By Proposition 3.2, any rational ring, $\mathbf{R}'$, with $\mathbf{R}' > \mathbf{R}$ has unit sum number 2.

We now investigate rational rings which have only two symbols ∞ within their types. Because of the importance of the prime 2, as illustrated in Proposition 2.1, we are in fact considering rings of the type $(\infty, r_2, r_3, \dots)$ where only a single r_i is ∞, the rest being zero. We begin with a technical lemma.

Lemma 3.4. *Let $a, b, c, d \in \mathbf{Z} \setminus \{0\}$ and let $(a/b), (c/d)$ be rational numbers expressed in lowest form. If $[(a/b) + (c/d)]$ is an integer, then $b = \pm d$.*

Proof. Straightforward.

Corollary 3.5. *Let $k, l, m, n \in \mathbf{Z}$. Let z be an integer, and let $p \neq 2$ be a rational prime such that $z = \pm(2^k p^l \pm 2^m p^n)$.*

If $k < 0$, or $m < 0$, then $k = m$. If $l < 0$, or $n < 0$, then $l = n$.

Proof. This follows directly from Lemma 3.4.

The following proposition provides a useful simplification in discussing the 2-sum property for all rational rings with only two symbols infinity in their type, one of which corresponds to the rational prime 2.

Lemma 3.6. *Let $p \in \Pi \setminus \{2\}$, and let $\mathbf{R}$ be the subring of $\mathbf{Q}$ generated by $1/2$ and $1/p$. Then $\operatorname{usn}(\mathbf{R}) = 2$ if and only if every positive integer z with $(z, 2) = 1 = (z, p)$ can be expressed in one of the following forms*:

(1) $z = \pm(2^k \pm p^l)$ *for some $k > 0$, $l > 0$.*

(2) $z = 2^k p^l \pm 1$ *for some $k > 0$, $l \geq 0$.*

(3) $z = (1/p^l)(2^k \pm 1)$ *for some $k > 0$, $l > 0$.*

(4) $z = (1/2^k)(p^l \pm 1)$ *for some $k > 0$, $l > 0$.*

where $k, l \in \mathbf{Z}$.

Proof. In the first direction we assume that $\operatorname{usn}(\mathbf{R}) = 2$. Every unit of $\mathbf{R}$ is of the form $\pm 2^a p^b$ where $a, b \in \mathbf{Z}$. Let z be a positive integer greater than 1 and relatively prime to both 2 and p. Let $z = \pm(2^a p^b \pm 2^c p^d)$ be a sum of two units for z where $a, b, c, d \in \mathbf{Z}$. Notice that a, b, c, d cannot all be less than or equal to zero since z cannot take the values $\pm 1, \pm 2$ or 0.

By Corollary 3.5, if $a < 0$ then $c = a$ and, since z is relatively prime to 2, then if either a or c is greater than 0, then the other must be zero, i.e., if $a > 0$, then $c = 0$. Similarly, if $b < 0$, then $d = b$, and since z is relatively prime to p, then if either b or d is greater than 0 then the other must be zero, i.e., of $b > 0$, then $d = 0$. In light of this, we consider the possible sums of two units for z.

If $a > 0$ (forcing $c = 0$) and $d > 0$ (forcing $b = 0$), then $z = \pm(2^a \pm p^d)$ This is of form **(1)**. Similarly, form **(1)** occurs for $c > 0$ and $b > 0$.

If $a > 0$ (forcing $c = 0$) and $b > 0$ (forcing $d = 0$), then $z = 2^a p^b \pm 1$. Note that only one $\pm$ sign occurs in this equation and it must accompany the 1, otherwise a negative integer would result. This equation is of form **(2)**. Similarly, form **(2)** occurs for $c > 0$ and $d > 0$. If $a = c < 0$, then $b > 0$ and $d = 0$ or $b = 0$ and $d > 0$ resulting in $z = (1/2^{-a})(p^b \pm 1)$ or $z = (1/2^{-a})(p^d \pm 1)$. Notice that there is only one $\pm$ sign in each equation and it must precede the 1, otherwise a negative integer would result. These equations are of form **(4)**.

If $b = d < 0$, then $a > 0$ and $c = 0$, or $a = 0$ and $c > 0$ resulting in $z = (1/p^{-b})(2^a \pm 1)$ or $z = (1/p^{-b})(2^c \pm 1)$. Again the only $\pm$ sign accompanies the 1 or a negative integer results. These equations are of form **(3)**.

If $b = d = 0$, then $a > 0$ and $c = 0$, or $a = 0$ and $c > 0$ resulting in $z = 2^a \pm 1$ or $z = 2^c \pm 1$. These equations are of form **(2)**.

We have covered all possible cases.

In the other direction let x be a positive integer. We can write $x = 2^a p^b(z)$ with $a, b \in \mathbf{Z}$ where $(z, 2) = 1 = (z, p)$ or $z = 1$. If $z(\neq 1)$ can be expressed in one of the forms **(1)**, **(2)**, **(3)** or **(4)** then, since $1 = (1/2) + (1/2)$, every positive integer can be expressed as unit $\cdot$ (unit + unit). Then, by Lemma 2.3, $\operatorname{usn}(\mathbf{R}) = 2$.

It is convenient for our purposes to consider the primes modulo 24. Excluding 2 and 3 the primes fall into eight classes modulo 24, those being 1, 5, 7, 11, 13, 17, 19 and 23 mod 24. By Dirichlet's famous theorem (see Prachar [**15**, IV, Theorem 4.3]) for primes in an arithmetic progression, we know that in each of these classes there is an infinite number of primes. Let P^* denote the set of primes $\{p \in \Pi \mid p \equiv 1, 5, 11, 13, 19 \text{ or } 23 \bmod 24\}$.

Proposition 3.7. *Let* $P^*_{25} = P^* \setminus \{5, 13, 23, 29, 101\}$ *and* $p \in P^*_{25}$. *Let* $\mathbf{R}$ *be the subring of* $\mathbf{Q}$ *generated by* $1/2$ *and* $1/p$. *Then* 25 *cannot be expressed as a sum of two units in* $\mathbf{R}$, *i.e.,* $\operatorname{usn}(\mathbf{R}) > 2$.

Proof. Since $(25, p) = 1$ for all $p \in P^*_{25}$ and $(25, 2) = 1$, then, by Proposition 3.6, if 25 can be expressed as a sum of two units of $\mathbf{R}$, it must be expressible in one of the forms **(1)**, **(2)**, **(3)** or **(4)**.

Form (1). We tabulate modulo 24 values of $\pm 2^k \pm p^l$ for $k, l > 0$ and for all possible values of p in P^*.

In the following table 1 mod 24 occurs only for $\pm 2^k \equiv 2$ or -4 mod 24, which correspond to $\pm 2^k = 2$ or -4. However, $25 = 2 \pm p^l$ implies that $p = 23$, which is not contained in P^*_{25}; and $25 = -4 \pm p^l$ implies $p = 29$, which is not contained in P^*_{25}. Therefore, 25 does not occur in $\mathbf{R}$ as form **(1)**.

TABLE $\pm 2^k \pm p^l \bmod 24; k, l > 0, p \in P^*$.

$\pm p^l \bmod 24$

$\pm 2^k \bmod 24$	+	1	5	11	13	19	23
	2	3	7	13	15	21	**1**
	4	5	9	15	17	23	3
	8	9	13	19	21	3	7
	16	17	21	3	5	11	15
	-4	21	**1**	7	9	15	19
	-2	23	3	9	11	17	21

Form (2). This time we tabulate values of $2^k p^l$ modulo 24 for $k > 0, l \geq 0$ and for all values of p in P^*.

TABLE $2^k p^l \bmod 24; k > 0, l \geq 0, p \in P^*$.

$p^l \bmod 24$

$\pm 2^k \bmod 24$	×	1	5	11	13	19	23
	2	**2**	10	22	**2**	14	22
	4	4	20	20	4	4	20
	8	8	16	16	8	8	16
	16	16	8	8	16	16	8

From this table we deduce that $2^k p^l \pm 1$ with $k > 0$ and $l \geq 0$ can only be congruent to 1 mod 24 for $k = 1$ (i.e., see values resulting in 0 or 2 in the table above). However, $25 = 2p^l \pm 1$ implies $p = 13$ which is not contained in P^*_{25}. Therefore 25 does not occur in $\mathbf{R}$ as form **(2)**.

Form (3). The set of congruences modulo 24 for $25p^l$ with $l > 0$ and $p \in P^*$ is $\{1, 5, 11, 13, 19, 23\}$. The set of congruences modulo 24 for $2^k \pm 1$ with $k > 0$ is $\{1, 3, 5, 7, 9, 15, 17\}$. Values common to both sets are 1 and 5 mod 24; these correspond to $k = 1$ and $k = 2$. Since

$25 > 2^k \pm 1$ for $k = 1$ or 2, then 25 cannot be expressed as form **(3)** in $\mathbf{R}$.

Form (4). The set of congruences modulo 24 for $25(2^k)$ with $k > 0$ is $\{2, 4, 8, 16\}$. The set of congruences modulo 24 for $p^l \pm 1$ with $l > 0$ and $p \in P^*$ is $\{0, 2, 4, 6, 10, 12, 14, 18, 20, 22\}$. Only the congruences 2 and 4 mod 24 occur in both sets. These correspond to $k = 1$ or 2. For $k = 1$ we get $2(25) = p^l \pm 1$ giving $p^l = 49$ or 51, both of which are impossible for $p \in P^*$. For $k = 2$ we get $4(25) = p^l \pm 1$ giving $p^l = 99$ or 101, neither of which is possible for $p \in P^*_{25}$. Therefore 25 cannot be expressed in form **(4)** in $\mathbf{R}$.

Proposition 3.8. *Let* $P^*_{73} = P^* \setminus \{37, 71, 293\}$ *and* $p \in P^*_{73}$. *If* $\mathbf{R}$ *is the subring of* $\mathbf{Q}$ *generated by* $1/2$ *and* $1/p$, *then* 73 *cannot be expressed as a sum of two units in* $\mathbf{R}$, *i.e.,* $\operatorname{usn}(\mathbf{R}) > 2$.

Proof. The proof follows Proposition 3.7 exactly, so we summarize just one form.

Form (1). Let $73 = 2 \pm p^l$ with $l > 0$ and $p \in P^*$. This implies $p = 71$ which is not contained in P^*_{73}.

Let $73 = -4 \pm p^l$ with $l > 0$ and $p \in P^*$. This implies that $77 = p^l$ which is impossible for $p \in P^*$. Therefore, 73 cannot be of form **(1)** in $\mathbf{R}$.

Corollary 3.9. *Let* $p \in P^*$, *and let* $\mathbf{R}$ *be the subring of* $\mathbf{Q}$ *generated by* $1/2$ *and* $1/p$. *Then* $\operatorname{usn}(\mathbf{R}) > 2$.

Proof. Recall from Propositions 3.7 and 3.8 that $P^*_{25} = P^* \setminus \{5, 13, 23, 29, 101\}$ and $P^*_{73} = P^* \setminus \{37, 71, 293\}$. Therefore, $P^* = P^*_{25} \cup P^*_{73}$. The proof then follows directly from these two propositions.

Theorem 3.10. *Let* $p \in \Pi \setminus \{2\}$, *and let* $\mathbf{R}$ *be the subring of* $\mathbf{Q}$ *generated by* $1/2$ *and* $1/p$. *Then* $\operatorname{usn}(\mathbf{R}) > 2$.

Proof. We consider p congruent to 7 mod 24, 17 mod 24 and finally $p = 3$. The proof is based on arithmetic arguments similar to those above. Then, using Corollary 3.9, the results follows; full details may be found in Meehan [**12**, III].

If $\mathcal{P}$ is a proper subset of Π containing 2 and at least one other prime, then we have the following analogue of the reduction Lemma 3.6.

Proposition 3.11. *Let* $\{2\} \subsetneq \mathcal{P} \subsetneq \Pi$. *Let* $\mathbf{R}$ *be the subring of* $\mathbf{Q}$ *generated by* $\{(1/p) \mid p \in \mathcal{P}\}$. *Then* $\operatorname{usn}(\mathbf{R}) = 2$ *if and only if every positive integer* z *with* $(z, p) = 1$ *for all* $p \in \mathcal{P}$ *can be expressed in one of the following forms*:

(a) $a = 1/(2^m B)(C \pm D)$

(b) $z = \pm(1/B)(2^m C \pm D)$

where $m \in \mathbf{N}$ *and* B, C, D *are products of elements of* $\mathcal{P} \setminus \{2\}$ *such that* $(B, C) = 1 = (C, D) = (B, D)$.

Proof. The proof is similar to that of Lemma 3.6. For full details, see Meehan [**12**].

Corollary 3.12. *Let* $\mathbf{R}$ *be the subring of* $\mathbf{Q}$ *generated by* $\{1/2\} \cup \{(1/p) \mid p \in \Pi, p \equiv 1 \bmod 24\}$. *Then* $\operatorname{usn}(\mathbf{R}) > 2$.

Proof. Consider the set $\mathcal{P} = \{2\} \cup \{p \in \Pi \mid p \equiv 1 \bmod 24\}$, and let $z = 11$. Then z is not of the form (a) since

$$(C \pm D) \equiv 0 \text{ or } 2 \bmod 24 \text{ and } 2^m \cdot 11B \equiv 22, 20, 16 \text{ or } 8 \bmod 24.$$

Moreover, z is not of form (b), either since

$$11B \equiv 11 \bmod 24 \quad \text{and} \quad \pm(2^m C \pm D) \equiv \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 15 \text{ or } \pm 17 \bmod 24.$$

Therefore by Proposition 3.11, $\operatorname{usn}(\mathbf{R}) \neq 2$.

By Dirichlet's theorem (see [**15**, IV, Theorem 4.3]), the set $\{p \in \Pi \mid p \equiv 1 \bmod 24\}$ is infinite and coinfinite and so the ring $\mathbf{R}$ in Corollary

3.12 is an example of a rational ring having endomorphism ring $\mathbf{R}$ with $\Pi \setminus X_R$ infinite but $\operatorname{usn}(\mathbf{R}) \neq 2$. In the next section we shall see that $\operatorname{usn}(\mathbf{R})$ is finite.

4. A number theoretical approach. A different line of approach is followed now adapting some results from additive number theory to get some interesting outcomes. We begin by recalling some fundamental notions and results; further background material may be found in Nathanson [**13**].

Definitions 4.1. Let A be a set of integers, $x \in \mathbf{Z}$ and $h \in \mathbf{N}$.

(i) The *Counting Function* of the set A, defined for $x \in \mathbf{Z}$, is the number of positive elements of A not exceeding x, written $A(x)$,

$$A(x) = \sum_{\substack{a \in A \\ 1 \leq a \leq x}} 1.$$

(ii) The *Shnirel'man Density* of the set A, denoted $\sigma(A)$, is

$$\sigma(A) = \inf_{n=1,2,\ldots} \left(\frac{A(n)}{n} \right)$$

(iii) *The set A is a basis of order h if every nonnegative integer can be expressed as a sum of exactly h elements of A.*

We include here some results which will be used later.

Lemma 4.2. *Let x be a positive integer greater than 2. Let $r(N)$ denote the number of representations of the integer N as the sum of two primes. Then*

(i) $\sum_{N \leq x} r(N) > c_1[x^2/(\ln x)^2]$, *for some positive constant c_1.*

(ii) $\sum_{N \leq x} (r(N))^2 \leq c_2[x^3/(\ln x)^4]$, *for some positive constant c_2.*

Proof. See Nathanson [**13**, Lemmas 7.6, 7.7].

Lemma 4.3. *Let A and B be sets of integers such that $0 \in A, 0 \in B$.*

(i) *If $n \in \mathbf{N}$ and $A(n) + B(n) \geq n$, then $n \in A + B$.*

(ii) *If $\sigma(A) + \sigma(B) \geq 1$, then $n \in A + B$ for each $n \in \mathbf{N}$.*

(iii) *If $\sigma(A) > 1/2$, then A is a basis of order 2.*

Proof. For (i) and (ii), see Nathanson [**13**, Lemmas 7.3, 7.4]; (iii) follows immediately from (ii) taking $A = B$.

Theorem 4.4 (Shnirel'man). *Let A and B be sets of integers such that $0 \in A$, $0 \in B$. Let $\sigma(A) = \alpha$ and $\sigma(B) = \beta$. Then $\sigma(A + B) \geq \alpha + \beta - \alpha\beta$.*

Proof. See Nathanson [**13**, Theorem 7.5].

Theorem 4.5. *Let $h \geq 1$ and let $A_1, \ldots, A_h$ be sets of integers such that $0 \in A_i$ for $i \in 1, \ldots, h$. Then*

$$1 - \sigma(A_1 + \cdots + A_h) \leq \prod_{i=1}^{h} (1 - \sigma(A_i)).$$

Proof. The proof is by induction on h. Let $\sigma(A_i) = \alpha_i$ for $i = 1, \ldots, h$. For $h = 1$ there is nothing to prove. For $h = 2$, the inequality follows from Theorem 4.4.

Let $k \geq 3$ and assume the theorem holds for all $h < k$. Let $B = A_1 + \cdots + A_{k-1}$. It follows from the induction hypothesis that $1 - \sigma(B) = 1 - \sigma(A_1 + \cdots + A_{k-1}) \leq \prod_{i=1}^{k-1} (1 - \sigma(A_i))$, and so

$$\begin{aligned} 1 - \sigma(A_1 + \cdots + A_k) &= 1 - \sigma(B + A_k) \\ &\leq (1 - \sigma(B))(1 - \sigma(A_k)) \qquad \text{(by Theorem 4.4)} \\ &\leq (1 - \sigma(A_k)) \prod_{i=1}^{k-1} (1 - \sigma(A_i)) \\ &= \prod_{i=1}^{k} (1 - \sigma(A_i)). \end{aligned}$$

This completes the proof.

The following theorem is fundamental to our line of approach.

Theorem 4.6 (Shnirel'man). *Let A be a set of integers such that $0 \in A$ and $\sigma(A) = \alpha > 0$. Then A is a basis of finite order. Further, A is a basis of finite order at most $h = 2l$, $h, l \in \mathbf{N}$ where l is defined by*

$$0 \leq (1-\alpha)^l \leq 1/2.$$

Proof. Let $\sigma(A) = \alpha > 0$. Then $0 \leq 1 - \alpha < 1$ and so $0 \leq (1-\alpha)^l \leq 1/2$ for some integer $l \geq 1$. By Theorem 4.5, $1 - \sigma(lA) \leq (1 - \sigma(A))^l = (1-\alpha)^l \leq 1/2$ and so $\sigma(lA) \geq 1/2$. Let $h = 2l$. It follows from Lemma 4.3(iii) that the set lA is a basis of order 2 and so A is a basis of order $2l = h$. This completes the proof.

Theorem 4.7 (Shnirel'man-Goldbach). *The set $A = \{0,1\} \cup \{p + q \mid p, q \in \Pi\}$ has positive Shnirel'man density.*

Proof. See [**13**, Theorem 7.8].

Recall that if $\mathcal{S}$ is a subset of Π and $\mathcal{S}(x)$ denotes the set of primes in $\mathcal{S}$ not exceeding x, then $\mathcal{S}$ is said to contain a positive proportion of Π provided $\mathcal{S}(x) > \theta\pi(x)$ for some real number $\theta \geq 0$ and all sufficiently large $x \in \mathbf{Z}$.

Lemma 4.8. *Let $\mathcal{S}$ be a subset of Π which contains a positive proportion of Π, then the set $\mathcal{S} \cup \{0,1\}$ is a basis of finite order.*

Proof. We show that the set $\mathcal{A} = \{0,1\} \cup \{p+q; p, q \in \mathcal{S}\}$ has positive Shnirel'man density. For any positive integer N let $r_{\mathcal{S}}(N)$ denote the number of representations of N as a sum of two primes belonging to $\mathcal{S}$. Then for all sufficiently large $x \in \mathbf{Z}$,

$$\sum_{N \leq x} r_{\mathcal{S}}(N) \geq \left(\mathcal{S}\left(\frac{x}{2}\right)\right)^2 \geq \left(\theta\pi\left(\frac{x}{2}\right)\right)^2,$$

and by the Prime Number theorem (see [**15**, III, Theorem 2.4])

$$\left(\theta\pi\left(\frac{\pi}{2}\right)\right)^2 \geq c_1\left(\frac{x/2}{\ln(x/2)}\right)^2, \quad \text{for some positive constant } c_1.$$

Also, by Lemma 4.2 (ii),

$$\sum_{N\leq x}(r_{\mathcal{S}}(N))^2 \leq c_2\frac{x^3}{(\ln x)^4}, \quad \text{for some positive constant } c_2.$$

Now by the Cauchy-Schwarz inequality (see [**13**, Lemma 7.1]),

$$\left(\sum_{N\leq x}(r_{\mathcal{S}}(N)\right)^2 \leq \sum_{\substack{N\leq x\\ r_{\mathcal{S}}(N)\geq 1}} 1 \sum_{N\leq x}(r_{\mathcal{S}}(N))^2.$$

Of course, $\sum_{N\leq x; r_{\mathcal{S}}(N)\geq 1} 1 \leq \mathcal{A}(x)$. Therefore, we can write

$$\frac{\mathcal{A}(x)}{x} \geq \frac{1}{2}\frac{(\sum_{N\leq x} r_{\mathcal{S}}(N))^2}{\sum_{N\leq x}(r_{\mathcal{S}}(N))^2},$$

and so

$$\frac{\mathcal{A}(x)}{x} \geq \frac{1}{x}\frac{(c_1[(x/2)/(\ln x/2)]^2)^2}{c_2[x^3/(\ln x)^4]} = \frac{c_1^2(\ln x)^4}{c_2(\ln x - \ln 2)^4} \geq \frac{c_1^2(\ln x)^4}{c_2(\ln x)^4}.$$

This means that $\mathcal{A}(x) \geq c_3 x$ for some positive constant c_3 and, for all sufficiently large x. Since $1 \in \mathcal{A}$ it follows that $\mathcal{A}$ has positive Shnirel'man density and so is a basis of finite order, say $h \in \mathbf{N}$. Therefore, every nonnegative integer can be expressed as a sum of exactly h elements of $\mathcal{A}$. Whenever 0 occurs in such a sum we may write $0+0$ and whenever 1 occurs, we may write $1+0$ and so any sum of exactly h elements of $\mathcal{A}$ is a sum of exactly $2h$ elements of $\mathcal{S}\cup\{0,1\}$. Therefore, $\mathcal{S}\cup\{0,1\}$ is a basis of order $2h$.

Theorem 4.9. *Let S be a subset of Π which contains a positive proportion of Π. If $2 \in S$, then $\mathbf{R}$, the subring of $\mathbf{Q}$ generated by $\{(1/p) \mid p \in S\}$ has finite unit sum number.*

Proof. By Lemma 4.8, the set $S \cup \{0,1\}$ is a basis of finite order, say of order $h \in \mathbf{N}$. For an arbitrary element r of $\mathbf{N}$,we have

$$r = s_1 + s_2 + \cdots + s_h, \quad s_i \in S \cup \{0,1\}, i = 1, \ldots, h.$$

If $s_i \in S \cup \{1\}$ for all $i = 1, \ldots, h$, then r is a sum of h units of $\mathbf{R}$.

If $s_1, \ldots, s_k \neq 0$ for some $1 \leq k < h$ and $s_{k+1}, \ldots, s_h = 0$, then

$$r = \sum_{i=1}^{k-1} s_i + s_k \left(\frac{1}{2^{h-k}} + \sum_{j=1}^{h-k} \frac{1}{2^j} \right)$$

is a sum of h units of $\mathbf{R}$. By Lemma 2.3, $\mathbf{R}$ has the h-sum property. So, certainly $\operatorname{usn}(\mathbf{R}) \leq h$.

This is a significant result. For example, letting $\Pi = \{p_i\}_{i=1,2,\ldots}$ under the natural ordering, the ring generated by $\{(1/p_1), (1/p_n), (1/p_{2n}), \ldots, (1/p_{in}), \ldots\}$ has finite unit sum number whatever $n \in \mathbf{N}$. (Note $\mathbf{R} = \mathbf{Q}$ for $n = 1$.)

From the Prime Number theorem (see [**15**, III, Theorem 2.4]) and the Prime Number theorem for arithmetic progressions (see [**15**, IV, Theorem 7.5]) we have that $\lim_{x\to\infty}(\pi(x,k,l)/\pi(x)) = (1/\varphi(k))$, where φ is the Euler function. So for any $\varepsilon > 0$, we can find $x_0 \in \mathbf{R}$ such that for all $x > x_0$ we have $-\varepsilon < (\pi(x,k,l)/\pi(x)) - (1/\varphi(k)) < \varepsilon$ and so $\pi(x,k,l) > \pi(x)[(1/\varphi(k)) - \varepsilon]$.

Now set $k = 24$, $l = 1$ and choose $\varepsilon = (1/16)$. Then $\pi(x, 24, 1) > (1/16)\pi(x)$ for all $x > x_0$ for some $x_0 \in \mathbf{R}$. Therefore, the set of primes congruent to 1 mod 24 is a positive proportion of Π and, by Theorem 4.9 and Proposition 3.7 we have proved:

Corollary 4.10. *Let* $P = \{2\} \cup \{p \in \Pi \mid p \equiv 1 \bmod 24\}$. *Let* $\mathbf{R}$ *be the subring of* $\mathbf{Q}$ *generated by* $\{(1/p) \mid p \in P\}$. *Then* $\operatorname{usn}(\mathbf{R})$ *is finite but greater than* 2.

It is possible to extend this approach to obtain an upper bound for the unit sum number of the above ring $\mathbf{R}$. Inevitably the bound so obtained is extravagantly large; it is shown in Meehan [**12**, III, Proposition 3.15] that 1208000 is an upper bound.

REFERENCES

1. R. Baer, *Abelian groups without elements of finite order*, Duke Math. J. **3** (1937), 68–122.

2. F. Castagna, *Sums of automorphisms of a primary abelian group*, Pacific J. Math. **27** (1968), 463–473.

3. A.L.S. Corner, *Every countable reduced torsion-free ring is an endomorphism ring*, Proc. London Math. Soc. (3) **13** (1963), 687–710.

4. A.L.S. Corner and R. Göbel, *Prescribing endomorphism algebras–a unified treatment*, Proc. London Math. Soc. (3) **50** (1985), 447–479.

5. H. Freedman, *On endomorphisms of primary abelian groups*, J. London Math. Soc. **43** (1968), 305–307.

6. L. Fuchs, *Infinite abelian groups* I, Academic Press, New York, 1970.

7. ———, *Infinite abelian groups* II, Academic Press, New York, 1973.

8. ———, *Recent results and problems on abelian groups*, Topics in Abelian Groups, Chicago, 1963, 9–40.

9. R. Göbel and A. Opdenhövel, *Every endomorphism of a local Warfield module of finite torsion-free rank is the sum of two automorphisms*, J. Algebra **233** (2000), 758–771.

10. B. Goldsmith, S. Pabst and A. Scott, *Unit sum numbers of rings and modules*, Quart. J. Math. Oxford **49** (1998), 331–344.

11. P. Hill, *Endomorphism rings generated by units*, Trans. Amer. Math. Soc. **141** (1969), 99–105.

12. C. Meehan, *Unit sum numbers of abelian groups and modules*, Ph.D. Thesis, Dublin Institute of Technology, 2001.

13. M.B. Nathanson, *Additive number theory: The classical bases*, Graduate Texts in Math. 164, Springer-Verlag, New York, 1996.

14. A. Opdenhövel, *Über Summen zweier Automorphismen von Moduln*, Ph.D. Thesis, Universität Essen, 1999.

15. K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.

16. L. Strüngmann, *Does the automorphism group generate the endomorphism ring in Rep(S, R)?*, J. Algebra **231** (2000), 163–179.

17. C. Wans, *Summen von Automorphismen für Moduln*, Thesis, Universität Essen, 1995.

18. D. Zelinsky, *Every linear transformation is a sum of nonsingular ones*, Proc. Amer. Math. Soc. **5** (1954), 627–630.

School of Mathematical Sciences, Dublin Institute of Technology, Kevin Street, Dublin 8, Ireland
E-mail address: brendan.goldsmith@dit.ie

School of Mathematical Sciences, Dublin Institute of Technology, Kevin Street, Dublin 8, Ireland
E-mail address: mcandt@gofree.indigo.ie

Fachbereich 6, Mathematik und Informatik, Universität Essen, 45117 Essen, Germany
E-mail address: simone.wallutis@uni-essen.de