Journal of Number Theory 171 (2017) 284–300

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On universal zero-free ternary quadratic form representations of primes in arithmetic progressions

Werner Hürlimann

Swiss Mathematical Society, CH-1700 Fribourg, Switzerland

ARTICLE INFO

Article history:
Received 12 May 2016
Accepted 26 July 2016
Available online 6 September 2016
Communicated by D. Goss

MSC:
11E25
11E41
11Y11
11Y50

Keywords:
Ternary quadratic form
Prime
Theorem of Gauss
Class number
Fundamental discriminant

ABSTRACT

For the specific set of fifteen ternary quadratic forms $x^2 + by^2 + cz^2$, $b, c \in \{1, 2, 4, 8\}$, $(b, c) \in \{(2, 16), (8, 16), (1, 3), (2, 3), (1, 5)\}$, it is shown that the distinct zero-free representations of an odd prime by these forms depend upon the class numbers $h(-kp)$, $k \in \{1, 3, 4, 5, 8, 12, 20, 24\}$. We determine when such a form is *universal zero-free* for an arithmetic progression of primes, i.e., when a prime from such a progression can be represented without zero components. The exceptional primes, which cannot be represented in this way, fall into two distinct classes. They are either infinite in number and belong to arithmetic progressions of primes, so-called *infinite exceptional sets*, or they are finite in number and build so-called *finite exceptional sets*. These exceptional sets are determined. Moreover, we show how to derive the finite number of primes expressible by a form $x^2 + by^2 + cz^2$ in essentially m ways, and illustrate the method. Reinterpreting results by Dirichlet [12], Dickson [10] and Kaplansky [23], we show that the forms $(b, c) \in \{(1, 2), (1, 3), (2, 3), (2, 4)\}$ are the only *strictly universal zero-free* forms of type $x^2 + by^2 + cz^2$, i.e., they can be represented without zero components for all primes up to a known finite number of primes.

E-mail address: whurlimann@bluewin.ch.

http://dx.doi.org/10.1016/j.jnt.2016.07.014
0022-314X/

1. Introduction

An important and very active topic of number theory concerns the representation of numbers by the positive ternary quadratic forms $ax^2 + by^2 + cz^2$, $1 \leq a \leq b \leq c$, also denoted by (a, b, c). From a historical perspective, the representations may include zeros, and permutations as well as sign changes of representations are viewed as different. A cornerstone of the classical theory of these forms is the theorem of Legendre–Gauss, which states that sums of three squares represent exactly all positive integers not of the form $4^k(8m + 7)$. Dirichlet [12] gave an elegant proof of this theorem (e.g. Dickson [9], pp. 263–264) and also proved that the form $(1, 1, 3)$ represents all positive integers not divisible by 3. Dickson [10] showed that the forms $(1, 1, 2)$, $(1, 2, 3)$ and $(1, 2, 4)$ represent all odd positive integers. Later on, Kaplansky [23] proved that there are no other such ternary forms (see also Panaitopol [27]). Williams [38] determines the 28 forms (a, b, c) that represent all positive integers $n \equiv 4 \pmod 8$ under the assumption of the Generalized Riemann Hypothesis. Williams [39] determines the 9 forms that represent all positive integers $n \equiv 2 \pmod 4$.

Although the form $(1, 1, 2)$ represents all odd positive integers, some of them cannot be represented with three non-zero squares. Examples are the primes 5, 11, 17, 29, 41, which belong to the arithmetic progressions of primes $p \equiv 1, 3, 5 \pmod 8$. On the other hand, all primes in the arithmetic progression $p \equiv 7 \pmod 8$ can be represented by this form using non-zero squares. Being interested in such zero-free representations of primes by positive ternary quadratic forms of type $(1, b, c)$, it is useful to introduce some terminology. An *arithmetic progression of primes* with initial term r and modulus m is a set of primes satisfying the congruence $p \equiv r \pmod m$, i.e., such that $p = km + r$ for some $k \geq 0$. The whole set of such primes is denoted by $P(r, m)$. For a fixed form $(1, b, c)$ we assume that a prime p satisfies $p \geq 1 + b + c$, a necessary condition for a zero-free representation of primes. When not mentioned explicitly, this condition is tacitly assumed.

Definitions 1.1. A set $P(r, m)$ is *universal zero-free* for the ternary quadratic form $(1, b, c)$ if every prime $p \in P(r, m)$, $p \geq 1 + b + c$, is of the form $p = x^2 + by^2 + cz^2$, $xyz \neq 0$. A form $(1, b, c)$ is *strictly universal zero-free* if all primes p, with the exception of finitely many of them, are of the form $p = x^2 + by^2 + cz^2$, $xyz \neq 0$ (independently of arithmetic progressions). If a form $(1, b, c)$ is not strictly universal zero-free there is some arithmetic progression of primes $P(r, m)$ such that infinitely many $p \in P(r, m)$ are not of the form $p = x^2 + by^2 + cz^2$, $xyz \neq 0$.

For the above form $(1, 1, 2)$ the set $P(7, 8)$ is universal zero-free, but the sets $P(r, 8)$, $r \in \{1, 3, 5\}$, are not universal zero-free, the exceptional primes being 17, 41 for $P(1, 8)$, 11 for $P(3, 8)$, and 5, 29 for $P(5, 8)$, as shown in the later Table 3.1. Moreover, this form is strictly universal zero-free. On the other hand, for the simplest form $(1, 1, 1)$, i.e., a sum of three squares, the sets $P(r, 8), r \in \{1, 3\}$ are universal zero-free, but $P(5, 8)$ is

not, the exceptional primes being 5, 13, 37, as follows from Table 3.1. Furthermore, the form $(1,1,1)$ is not strictly universal zero-free because none of the primes $p \in P(7,8)$ are represented by sums of three squares (theorem of Legendre–Gauss). These two examples suggest that for a more precise and complete classification of primes represented by a form $(1,b,c)$ some additional notions are required.

Definitions 1.2. An arithmetic progression of primes $P(r,m)$ is called an *infinite exceptional set* for the form $(1,b,c)$ if all primes $p \in P(r,m)$ cannot be represented by this form. A finite set of primes in $P(r,m)$ is called a *finite exceptional set* for the form $(1,b,c)$, denoted by $F(r,m)$, if the finitely many primes $p \in F(r,m)$, are the only primes in $P(r,m)$, $p \geq 1+b+c$, which are not of the form $p = x^2 + by^2 + cz^2$, $xyz \neq 0$.

The Definitions 1.1 and 1.2 allow for a complete classification of primes with respect to a zero-free representation by a form $(1,b,c)$ (see Theorem 3.1/Table 3.1). If a form is strictly universal zero-free, then there are no infinite exceptional sets but there may be some finite exceptional sets. By the mentioned theorems of Dirichlet [12], Dickson [10] and Kaplansky [23], it is clear that the forms $(1,1,2)$, $(1,1,3)$, $(1,2,3)$ and $(1,2,4)$ are the only possible strictly universal zero-free ternary quadratic forms. This unified result can be viewed as a zero-free extension of these classical theorems when restricted to odd primes.

The finite exceptional sets for these forms are given as follows (see the Table 3.1):

$$
\begin{aligned}
&(1,1,2): && F(1,8) = \{17,41\},\ F(3,8) = \{11\},\ F(5,8) = \{5,29\},\\
&(1,2,4): && F(1,8) = \{17,41\},\ F(3,8) = \{11\},\ F(5,8) = \{29\},\\
&(1,1,3): && F(7,24) = \{7,31\},\ F(19,24) = \{19\},\\
&(1,2,3): && F(1,24) = \{73\},\ F(11,24) = \{11,83\},\ F(19,24) = \{19,43\},\\
& && F(r,24) = \{r\}, r \in \{7,13,17\}.
\end{aligned}
$$

All other forms of type $(1,b,c)$ are not strictly universal zero-free. For each of them, there is at least one infinite exceptional set $P(r,m)$. Moreover, the remaining primes in arithmetic progressions, which are not infinite exceptional sets, fall into distinct universal zero-free and/or finite exceptional sets. Some examples of forms, taken from Table 3.1, illustrate this fact:

$(1,1,1)$: $P(7,8)$ is the infinite exceptional set,
$P(1,8)$ and $P(3,8)$ are the universal zero-free sets,
$F(5,8) = \{5,13,37\}$ is the finite exceptional set,

$(1,1,8)$: $P(3,8)$ and $P(7,8)$ are the infinite exceptional sets,
$F(1,8) = \{17,41\}$ and $F(5,8) = \{29\}$ are the finite exceptional sets, there is no universal zero-free set,

$(1,2,2)$: $P(7,8)$ is the infinite exceptional set,
$P(r,8) = \{r\}$, $r \in \{1,3,5\}$, are the universal zero-free sets, there is no finite exceptional set.

A brief summary of the content follows.

The preliminary Section 2 reviews essential material on counting functions of ternary quadratic forms required in the subsequent analysis. If one denotes by $R^d_{(1,b,c)}(n)$ the number of distinct zero-free representations of a given number n by a positive ternary quadratic form $(1, b, c)$, then Theorem 2.1 recalls the general expressions for its evaluation. Specialization to the case $n = p$ of prime numbers follows. The considered fifteen pairs of values $1 \leq b \leq c$ have all the property that the corresponding counting formulas $R^d_{(1,b,c)}(p)$ depend on the number $h(D)$ of classes of binary quadratic forms with negative fundamental discriminant D associated to primes in arithmetic progressions. Of first importance is the theorem of Gauss, which enables to express $R^d_3(p) = R^d_{(1,1,1)}(p)$ in terms of the class numbers $h(-p)$ and $h(-4p)$. Similarly, the counting functions $R^d_{(1,b,c)}(p)$ of the Bell forms $(1, b, c)$ with $b, c \in \{1, 2, 4, 8\}$, and the generalized Bell forms with $(b, c) \in \{(2, 16), (8, 16)\}$, are functions of $h(-p)$, $h(-4p)$ and $h(-8p)$ (Theorem of Bell [3], Hürlimann [20], Theorems 2.1 and 3.1). Presumably, the counting function $R^d_{(1,b,c)}(p)$ of other forms will share a similar property. For example, the form $(1, 1, 3)$ can be expressed in terms of $h(-3p)$ and $h(-12p)$ in virtue of the Conjecture 18 of Sun [32], which has been proved by Guo et al. [17]. Corollary 2.1 lists the class number conditions required to solve the equation $R^d_{(1,b,c)}(p) = m \geq 0$ for all the considered fifteen forms $(1, b, c)$. Then, Section 3 presents the detailed analysis of the universal zero-free property (Definitions 1.1) and a description of the infinite and finite exceptional sets (Definitions 1.2) for the fifteen ternary quadratic forms $(1, b, c)$. Section 4 proposes a classification of the zero-free prime representations by ternary quadratic forms in essentially m ways and illustrate it for sums of three squares.

2. Zero-free representations of primes by some ternary quadratic forms

In classical arithmetic, given a quadratic form $Q(x_1, x_2, ..., x_k)$, one is interested in representing a number n by this form, i.e., in integer solutions of the Diophantine equation $Q(x_1, x_2, ..., x_k) = n$. The number of such representations, counting zeros, permutations and sign changes, is denoted by $r_Q(n)$. This, and the total number of primitive solutions only, denoted by $R_Q(n)$, are related by the formula $r_Q(n) = \sum_{d^2|n} R_Q(\frac{n}{d^2})$, which can be inverted using Möbius inversion, if necessary (e.g. Cooper and Hirschhorn [7], Eq. (1.3)). In the important special case of sums of $k \geq 2$ squares with $Q(x_1, x_2, ..., x_k) = x_1^2 + x_2^2 + \cdots + x_k^2$, the standard notations $r_k(n)$ and $R_k(n)$ are of common use. In general, one is also interested in the number $R^d_Q(n)$ of distinct primitive representations of n by the quadratic form $Q(x_1, x_2, ..., x_k)$ without zeros such that $\prod_{j=1}^k x_j \neq 0$. In case $Q(x_1, x_2, ..., x_k) = x_1^2 + x_2^2 + \cdots + x_k^2$ the notation $R^d_k(n)$ is used.

Clearly, the number $R^d_Q(n)$ depends upon $R_Q(n)$, which is called *principal component* of $R^d_Q(n)$. For combinatorial reasons, a formula for $R^d_Q(n)$ will also depend upon other *auxiliary components* $R^d_{Q'}(n)$ for various other quadratic forms Q' or degree less than k. For example, the number of primitive quadruples $R^d_3(t^2)$ depends besides the principal ternary component $R_3(t^2)$ on the auxiliary binary components $R^d_{Q_1}(t^2)$ and $R^d_{Q_2}(t^2)$ with $Q_1(x_1, x_2) = x_1^2 + x_2^2$ and $Q_2(x_1, x_2) = x_1^2 + 2x_2^2$ respectively (e.g. Hürlimann [18]).

In the present work, we study the number $R_Q^d(p)$, p and odd prime number, for some ternary diagonal quadratic forms $Q(x,y,z) = x^2 + by^2 + cz^2$ with $1 \leq b \leq c$. Instead of $r_Q(n)$, $R_Q(n)$ and $R_Q^d(n)$ we use the notations $r_{(1,b,c)}(n)$, $R_{(1,b,c)}(n)$ and $R_{(1,b,c)}^d(n)$. In the process of finding formulas for $R_{(1,b,c)}^d(n)$, one is led to consider also the number of distinct primitive solutions of $Q(x_1, x_2, ..., x_k) = n$ with $\prod_{j=1}^k x_j \neq 0$ and two-by-two different entries $x_i \neq x_j$, $1 \leq i < j \leq k$, a counting function denoted by $D_Q(n)$. In particular, for the binary quadratic forms $Q(x,y;a,b) = ax^2 + by^2$ we use the notation $D_Q(n) = D_{(a,b)}(n)$. Moreover, the notational convention $D_2(n) = D_{(1,1)}(n)$ is made. General expressions for the evaluation of $R_{(1,b,c)}^d(n)$ are summarized in the following basic result.

Theorem 2.1. *The number of distinct zero-free primitive representations of a number $n \geq 1 + b + c$ by the forms $x^2 + by^2 + cz^2$, $1 \leq b \leq c$, satisfies the following parametric formulas:*

$$48R_3^d(n) = R_3(n) + 24D_{(1,2)}(n) - 24D_2(n), \quad (b,c) = (1,1), \tag{2.1}$$

$$16R_{(1,1,2)}^d(n) = R_{(1,1,2)}(n) + 16D_{(2,2)}(n) - 8D_2(n) - 8D_{(1,2)}(n), \quad (b,c) = (1,2), \tag{2.2}$$

$$16R_{(1,1,c)}^d(n) = R_{(1,1,c)}(n) + 8D_{(2,c)}(n) - 8D_2(n) - 8D_{(1,c)}(n), \quad 1 = b, 2 < c, \tag{2.3}$$

$$16R_{(1,b,b)}^d(n) = R_{(1,b,b)}(n) + 8D_{(1,2b)}(n) + 16D_{(b,1+b)}(n) - 8D_{(1,b)}(n) - 8D_{(b,b)}(n), \quad 1 < b = c, \tag{2.4}$$

$$8R_{(1,b,c)}^d(n) = R_{(1,b,c)}(n) - 4D_{(1,b)}(n) - 4D_{(1,c)}(n) - 4D_{(b,c)}(n), \quad 1 < b < c. \tag{2.5}$$

Proof. In the present form (2.1) is found in Hürlimann [21], formula (5). Some other formulas have been shown for the special case $n = t^2$ in Hürlimann [19]. In its full generality, Theorem 2.1 is shown in Hürlimann [22], Section 2. □

According to this result, the exact evaluation of any specific $R_{(1,b,c)}^d(n)$ requires explicit expressions for the right hand side counting functions in (2.1)–(2.5).

From now on, we specialize to the case $n = p$ of prime numbers. The considered values of $1 \leq b \leq c$ have all the property that the corresponding counting formulas $R_{(1,b,c)}^d(p)$ depend on the number $h(D)$ of classes of binary quadratic forms with negative fundamental discriminant D associated to primes in arithmetic progressions. Of first importance is the theorem of Gauss [14] (cf. Dickson [9], p. 262, Grosswald [16], Section 4.8, Theorem 2′, Rehm [29] for a modern proof, Bateman and Grosswald [2], Lemma 3), which states that for a square-free number n one has

$$R_3(n) = \begin{cases} 12h(-4n), & n > 1, n \equiv 1, 2, 5, 6 \mod 8, \\ 24h(-n), & n > 3, n \equiv 3 \mod 8, \\ 0, & n \equiv 7 \mod 8. \end{cases} \tag{2.6}$$

This result is very useful because for the Bell forms $(1, b, c)$ with $b, c \in \{1, 2, 4, 8\}$, and the generalized Bell forms with $(b, c) \in \{(2, 16), (8, 16)\}$ the counting function $R_{(1,b,c)}(n)$ depends only upon $R_3(n)$ (Bell [3] and Hürlimann [20], Theorems 2.1 and 3.1). Without further mention, frequent use will also be made of the binary quadratic formulas

$$D_2(p) = \frac{1}{2}\left(1 + \left(\frac{-1}{p}\right)\right), \quad D_{(1,2)}(p) = \frac{1}{2}\left(1 + \left(\frac{-2}{p}\right)\right), \quad D_{(2,2)}(p) = 0, \tag{2.7}$$

where $(\frac{\cdot}{p})$ denotes the symbol of Legendre. The first formula is found in Cooper and Hirschhorn [7], Eq. (1.6), the second one follows from Cox [8], Lemma 3.25, p. 55, and the third is trivial because p is an odd prime. The basic building block of the present study is the following result.

Theorem 2.2. *Let $p \geq 1 + b + c$ be an odd prime. Table 2.1 determines the number of distinct solutions of the Diophantine equation $p = x^2 + by^2 + cz^2$, $xyz \neq 0$, for the listed set of fifteen ternary quadratic forms $(1, b, c)$.*

The proof makes use of some auxiliary known congruence conditions about the representation of primes by binary quadratic forms. In particular, the following result will be repeatedly used.

Lemma 2.1. *For the given values of (a, b), the following necessary and sufficient conditions for the unique representation of primes p by the binary quadratic form $ax^2 + by^2$ hold:*

$$\begin{aligned}
&\text{(C1)} \quad (a,b) = (1,8) : p \equiv 1 \pmod 8 \\
&\text{(C2)} \quad (a,b) = (2,3) : p \equiv 5, 11 \pmod{24} \\
&\text{(C3)} \quad (a,b) = (4,5) : p \equiv 1, 9 \pmod{20} \\
&\text{(C4)} \quad (a,b) = (1,16) : p \equiv 1 \pmod 8 \\
&\text{(C5)} \quad (a,b) = (1,5) : p \equiv 1, 9 \pmod{20} \\
&\text{(C6)} \quad (a,b) = (2,5) : p \equiv 1, 9, 21, 29 \pmod{40}
\end{aligned}$$

Proof. All the congruence conditions follow from Sun and Williams [33], Lemma 9.2 and Table 9.1, pp. 159–160.

Proof of Theorem 2.2. To be represented by a form $(1, b, c)$ without zeros, one must have $p \geq 1 + b + c$. The formulas for the form $(1, 1, 1)$, i.e., for sums of three squares, follow easily by inserting (2.6)–(2.7) into (2.1) and taking into account the values of the Legendre symbols (note that $h(-p) = 1$ for $p = 3$). For the next eleven forms, the value of $R_{(1,b,c)}(p) = r_{(1,b,c)}(p)$ is taken from Hürlimann [21], Theorems 2.1 and 3.1. Based on Theorem 2.1 above the formulas are shown as follows.

Table 2.1
Class number formulas for the counting function $R^d_{(1,b,c)}(p)$.

Form	Arithmetic progression	Counting function	Form	Arithmetic progression	Counting function
$(1,1,1)$	$p \equiv 1 \pmod 8$	$\frac{1}{4}h(-4p)$	$(1,4,4)$	$p \equiv 1,9 \pmod{40}$	$\frac{1}{4}[h(-4p)+4]$
	$p \equiv 5 \pmod 8$	$\frac{1}{4}[h(-4p)-2]$		$p \equiv 17,25,33 \pmod{40}$	$\frac{1}{4}h(-4p)$
	$p \equiv 3 \pmod 8$	$\frac{1}{2}[h(-p)+1]$		$p \equiv 21,29 \pmod{40}$	$\frac{1}{4}[h(-4p)+2]$
	$p \equiv 7 \pmod 8$	0		$p \equiv 3 \pmod 4$	0
$(1,1,2)$ & $(1,2,4)$	$p \equiv 1 \pmod 8$	$\frac{1}{4}[h(-8p)-4]$	$(1,2,16)$	$p \equiv 1 \pmod 8$	$\frac{1}{4}[h(-8p)-4]$
	$p \equiv 3,5 \pmod 8$	$\frac{1}{4}[h(-8p)-2]$		$p \equiv 3 \pmod 8$	$\frac{1}{4}[h(-8p)-2]$
	$p \equiv 7 \pmod 8$	$\frac{1}{4}h(-8p)$		$p \equiv 5,7 \pmod 8$	0
$(1,1,4)$	$p \equiv 1 \pmod 4$	$\frac{1}{2}[h(-4p)-2]$	$(1,8,16)$	$p \equiv 1 \pmod 8$	$\frac{1}{4}[h(-8p)-4]$
	$p \equiv 3 \pmod 4$	0		$p \equiv 3,5,7 \pmod 8$	0
$(1,2,2)$	$p \equiv 1 \pmod 8$	$\frac{1}{4}h(-4p)$	$(1,1,3)$	$p \equiv 1 \pmod{24}$	$\frac{1}{4}[3h(-3p)-4]$
	$p \equiv 5 \pmod{24}$	$\frac{1}{4}[h(-4p)+6]$		$p \equiv 17 \pmod{24}$	$\frac{1}{4}[3h(-3p)-2]$
	$p \equiv 13,21 \pmod{24}$	$\frac{1}{4}[h(-4p)+2]$		$p \equiv 5 \pmod{24}$	$\frac{1}{2}h(-3p)$
	$p \equiv 11 \pmod{24}$	$\frac{1}{2}[3h(-p)+1]$		$p \equiv 13 \pmod{24}$	$\frac{1}{2}[h(-3p)-2]$
	$p \equiv 3,19 \pmod{24}$	$\frac{1}{2}[3h(-p)-1]$		$p \equiv 7,19 \pmod{24}$	$\frac{1}{8}[h(-12p)-4]$
	$p \equiv 7 \pmod 8$	0		$p \equiv 11 \pmod{24}$	$\frac{1}{8}[h(-12p)+4]$
				$p \equiv 23 \pmod{24}$	$\frac{1}{8}h(-12p)$
$(1,1,8)$ & $(1,4,8)$	$p \equiv 1 \pmod 8$	$\frac{1}{4}[h(-8p)-4]$	$(1,2,3)$	$p \equiv 1,11,19 \pmod{24}$	$\frac{1}{8}[h(-24p)-8]$
	$p \equiv 5 \pmod 8$	$\frac{1}{4}[h(-8p)-2]$		$p \equiv 5,7,13,17 \pmod{24}$	$\frac{1}{8}[h(-24p)-4]$
	$p \equiv 3 \pmod 4$	0		$p \equiv 23 \pmod{24}$	$\frac{1}{8}h(-24p)$
$(1,2,8)$	$p \equiv 1 \pmod 8$	$\frac{1}{2}[h(-4p)-2]$	$(1,1,5)$	$p \equiv 1,9,21,29 \pmod{40}$	$\frac{1}{8}[h(-20p)-8]$
	$p \equiv 3 \pmod 8$	$\frac{1}{2}[3h(-p)-1]$		$p \equiv 17,33 \pmod{40}$	$\frac{1}{8}[h(-20p)-4]$
	$p \equiv 5,7 \pmod 8$	0		$p \equiv 13,37 \pmod{40}$	$\frac{1}{8}h(-20p)$
$(1,8,8)$	$p \equiv 1 \pmod 8$	$\frac{1}{4}[h(-4p)+4]$		$p \equiv 31,39 \pmod{40}$	$\frac{1}{4}h(-5p)$
	$p \equiv 3,5,7 \pmod 8$	0		$p \equiv 7,23 \pmod{40}$	$\frac{1}{4}[h(-5p)+2]$
				$p \equiv 3 \pmod 8$	0

Forms (1, 1, 2) & (1, 2, 4)

For the form $(1,1,2)$, insert $R_{(1,1,2)}(p) = \frac{1}{3}R_3(2p) = 4h(-8p)$ into (2.2) to get $R^d_{(1,1,2)}(p) = \frac{1}{4}h(-8p) - \frac{1}{4}(1+(\frac{-1}{p})) - \frac{1}{4}(1+(\frac{-2}{p}))$, which implies the stated counting function taking into account the corresponding values of the Legendre symbol. Similarly, one has $R_{(1,2,4)}(p) = \frac{1}{6}R_3(2p) = 2h(-8p)$. Inserted into (2.5) yields the same counting function by noting that $D_{(1,4)}(p) = D_2(p) = \frac{1}{2}(1+(\frac{-1}{p}))$.

Form (1, 1, 4)

One has $R_{(1,1,4)}(p) = \frac{2}{3}R_3(p) = 8h(-4p)$ if $p \equiv 1 \pmod 4$ and $R_{(1,1,4)}(p) = 0$ otherwise. Inserting into (2.3) and using again that $D_{(1,4)}(p) = D_2(p)$ one obtains the result.

Forms (1, 1, 8) & (1, 4, 8)

First, one has $R_{(1,1,8)}(p) = \frac{1}{3}R_3(2p) = 4h(-8p)$ if $p \equiv 1 \pmod 4$ and $R_{(1,1,8)}(p) = 0$ otherwise. Inserted into (2.3) one gets $R^d_{(1,1,8)}(p) = \frac{1}{16}R_{(1,1,8)}(p) - \frac{1}{2}D_2(p) - \frac{1}{2}D_{(1,8)}(p)$.

Now, the binary quadratic form x^2+8y^2 represents an odd prime in one and only one way if, and only if, it belongs to the arithmetic progression $p \equiv 1 \pmod 8$ (condition (C1) of Lemma 2.1). With this, the stated counting function follows without difficulty. Similarly, one has $R_{(1,4,8)}(p) = \frac{1}{6}R_3(2p) = 2h(-8p)$ if $p \equiv 1 \pmod 4$ and $R_{(1,4,8)}(p) = 0$ otherwise. Inserted into (2.5) the same counting function follows.

Form (1, 2, 8)

For this form the theorem of Bell tells us that

$$R_{(1,2,8)}(p) = \begin{cases} \frac{1}{3}R_3(p), & p \equiv 1 \pmod 8 \\ \frac{1}{2}R_3(p), & p \equiv 3 \pmod 8 \\ 0, & p \equiv 5,7 \pmod 8 \end{cases} = \begin{cases} 4h(-4p), & p \equiv 1 \pmod 8, \\ 12h(-p), & p \equiv 3 \pmod 8, \\ 0, & p \equiv 5,7 \pmod 8. \end{cases}$$

The desired formula follows by inserting into (2.5) using that $D_{(1,8)}(p) = 1 \Leftrightarrow p \equiv 1 \pmod 8$.

Form (1, 2, 2)

Similarly to the preceding form, one has

$$R_{(1,2,2)}(p) = \begin{cases} \frac{1}{3}R_3(p), & p \equiv 1 \pmod 4 \\ R_3(p), & p \equiv 3 \pmod 8 \\ 0, & p \equiv 7 \pmod 8 \end{cases} = \begin{cases} 4h(-4p), & p \equiv 1 \pmod 4, \\ 24h(-p), & p \equiv 3 \pmod 8, \\ 0, & p \equiv 7 \pmod 8. \end{cases}$$

Inserted into (2.4) one sees that $R^d_{(1,2,2)}(p) = \frac{1}{16}R_{(1,2,2)}(p) + \frac{1}{2}D_{(1,4)}(p) + D_{(2,3)}(p) - \frac{1}{2}D_{(1,2)}(p)$. Condition (C2) of Lemma 2.1 implies that $D_{(2,3)}(p) = 1$ if $p \equiv 5, 11 \pmod{24}$ and $D_{(2,3)}(p) = 0$ otherwise. Now, a careful case by case analysis shows that $R^d_{(1,2,2)}(p)$ is determined by the formulas in Table 2.1.

Form (1, 4, 4)

One has $R_{(1,4,4)}(p) = \frac{1}{3}R_3(p) = 4h(-4p)$ if $p \equiv 1 \pmod 4$ and $R_{(1,4,4)}(p) = 0$ otherwise. Inserted into (2.4) one sees that $R^d_{(1,4,4)}(p) = \frac{1}{16}R_{(1,4,4)}(p) + \frac{1}{2}D_{(1,8)}(p) + D_{(4,5)}(p) - \frac{1}{2}D_{(1,4)}(p)$. Furthermore, as seen above one has $D_{(1,8)}(p) = 1 \Leftrightarrow p \equiv 1 \pmod 8$, and with condition (C3) of Lemma 2.1 one has $D_{(4,5)}(p) = 1$ if $p \equiv 1, 9 \pmod{20}$ and $D_{(4,5)}(p) = 0$ otherwise. A careful analysis implies the desired formulas.

Form (1, 8, 8)

One has $R_{(1,8,8)}(p) = \frac{1}{3}R_3(p) = 4h(-4p)$ if $p \equiv 1 \pmod 8$ and $R_{(1,4,4)}(p) = 0$ otherwise. Inserted into (2.4) one sees that $R^d_{(1,8,8)}(p) = \frac{1}{16}R_{(1,8,8)}(p) + \frac{1}{2}D_{(1,16)}(p) + D_{(8,9)}(p) - \frac{1}{2}D_{(1,8)}(p)$. From condition (C4) of Lemma 2.1 one gets $D_{(1,16)}(p) = 1$ if $p \equiv 1 \pmod 8$ and $D_{(1,16)}(p) = 0$ otherwise. On the other hand, the binary quadratic form $8x^2 + 9y^2$ with discriminant $d = -288$ is a reduced form with a single class in each genus (e.g. Dickson [11], Table I, p. 85), and since $8x^2 + 9y^2 = p \equiv 3, 5, 7 \pmod 8$ is

impossible, one sees that $D_{(8,9)}(p) = 1$ if $p \equiv 1 \pmod 8$ and $D_{(8,9)}(p) = 0$ otherwise. The desired formula follows.

Form (1, 2, 16)

For this generalized Bell ternary quadratic form one has $R_{(1,2,16)}(p) = \frac{1}{6}R_3(2p) = 2h(-8p)$ if $p \equiv 1, 3 \pmod 8$ and $R_{(1,2,16)}(p) = 0$ otherwise. Inserted into (2.5) one sees that $R^d_{(1,2,16)}(p) = \frac{1}{8}R_{(1,2,16)}(p) - \frac{1}{2}D_{(1,2)}(p) - \frac{1}{2}D_{(1,16)}(p)$, which implies the result taking into account that $D_{(1,16)}(p) = 1$ if $p \equiv 1 \pmod 8$ and $D_{(1,16)}(p) = 0$ otherwise ((C4) of Lemma 2.1).

Form (1, 8, 16)

For this generalized Bell form one has $R_{(1,8,16)}(p) = \frac{1}{6}R_3(2p) = 2h(-8p)$ if $p \equiv 1 \pmod 8$ and $R_{(1,2,16)}(p) = 0$ otherwise. From (2.5) one gets $R^d_{(1,8,16)}(p) = \frac{1}{8}R_{(1,8,16)}(p) - \frac{1}{2}D_{(1,8)}(p) - \frac{1}{2}D_{(1,16)}(p)$, which implies the result.

Form (1, 1, 3)

From the Conjecture 18 of Sun [32], which has been proved by Guo et al. [17], one knows that

$$R_{(1,1,3)}(p) = \begin{cases} 12h(-3p), & p \equiv 1 \pmod 8, \\ 8h(-3p), & p \equiv 5 \pmod 8, \\ 2h(-12p), & p \equiv 3 \pmod 4. \end{cases}$$

Note that Guo et al. [17] define $h(d)$ as the class number of the imaginary quadratic field $Q(\sqrt{d})$ while here $h(D)$ denotes the class number of the corresponding fundamental discriminant. One has $D = d$ if $d \equiv 1 \pmod 4$ and $D = 4d$ otherwise. Inserted into (2.3) one gets $R^d_{(1,1,3)}(p) = \frac{1}{16}R_{(1,1,3)}(p) + \frac{1}{2}D_{(2,3)}(p) - \frac{1}{2}D_2(p) - \frac{1}{2}D_{(1,3)}(p)$. From the proof for the form $(1, 2, 2)$ one knows that $D_{(2,3)}(p) = 1$ if $p \equiv 5, 11 \pmod{24}$ and $D_{(2,3)}(p) = 0$ otherwise. Furthermore, one knows that $D_{(1,3)}(p) = 1$ if $p \equiv 1 \pmod 3$ and $D_{(1,3)}(p) = 0$ otherwise (e.g. Dickson [11], Exercises XII, no. 3, p. 80). The result follows. □

Form (1, 2, 3)

With the method of Guo et al. [17], Section 6, and p. 247, one gets $R_{(1,2,3)}(p) = h(-24p)$. Inserted into (2.5) one obtains $R^d_{(1,2,3)}(p) = \frac{1}{8}R_{(1,2,3)}(p) - \frac{1}{2}D_{(1,2)}(p) - \frac{1}{2}D_{(1,3)}(p) - \frac{1}{2}D_{(2,3)}(p)$. One concludes as in the proof for the form $(1, 1, 3)$.

Form (1, 1, 5)

With the same method, one obtains also the following formula

$$R_{(1,1,5)}(p) = \begin{cases} 2h(-20p), & p \equiv 1 \pmod 4, \\ 4h(-5p), & p \equiv 7 \pmod 8, \\ 0, & p \equiv 3 \pmod 8. \end{cases}$$

Table 2.2
Class number conditions for solving the equation $R^d_{(1,b,c)}(p) = 0$.

Form	Arithmetic progression	Condition	Form	Arithmetic progression	Condition
$(1,1,1)$	$p \equiv 5 \pmod 8$	$h(-4p) = 2$	$(1,4,4)$	$p \equiv 3 \pmod 4$	none
	$p \equiv 7 \pmod 8$	none			
$(1,1,2)$& $(1,2,4)$	$p \equiv 1 \pmod 8$	$h(-8p) = 4$	$(1,8,8)$	$p \equiv 3,5,7 \pmod 8$	none
	$p \equiv 3,5 \pmod 8$	$h(-8p) = 2$			
$(1,1,4)$	$p \equiv 1 \pmod 4$	$h(-4p) = 2$	$(1,2,16)$	$p \equiv 1 \pmod 8$	$h(-8p) = 4$
	$p \equiv 3 \pmod 4$	none		$p \equiv 3 \pmod 8$	$h(-8p) = 2$
$(1,2,2)$	$p \equiv 7 \pmod 8$	none		$p \equiv 5,7 \pmod 8$	none
$(1,1,8)$ & $(1,4,8)$	$p \equiv 1 \pmod 8$	$h(-8p) = 4$	$(1,8,16)$	$p \equiv 1 \pmod 8$	$h(-8p) = 4$
	$p \equiv 5 \pmod 8$	$h(-8p) = 2$		$p \equiv 3,5,7 \pmod 8$	none
	$p \equiv 3 \pmod 4$	none			
$(1,2,8)$	$p \equiv 1 \pmod 8$	$h(-4p) = 2$	$(1,1,3)$	$p \equiv 13 \pmod{24}$	$h(-3p) = 2$
	$p \equiv 5,7 \pmod 8$	none		$p \equiv 7,19 \pmod{24}$	$h(-12p) = 4$
$(1,2,3)$	$p \equiv 1,11,19 \pmod{24}$	$h(-24p) = 8$	$(1,1,5)$	$p \equiv 1,9 \pmod{20}$	$h(-20p) = 8$
	$p \equiv 5,7,13,17 \pmod{24}$	$h(-24p) = 4$		$p \equiv 17,33 \pmod{40}$	$h(-20p) = 4$
				$p \equiv 3 \pmod 8$	none

Inserted into (2.3) one gets $R^d_{(1,1,5)}(p) = \frac{1}{16}R_{(1,1,5)}(p) + \frac{1}{2}D_{(2,5)}(p) - \frac{1}{2}D_2(p) - \frac{1}{2}D_{(1,5)}(p)$. With (C5) of Lemma 2.1, one has $D_{(1,5)}(p) = 1$ if $p \equiv 1,9 \pmod{20}$, $D_{(1,5)}(p) = 0$ otherwise, and similarly, with (C6) of Lemma 2.1, one has $D_{(2,5)}(p) = 1$ if $p \equiv 1,9,21, 29 \pmod{40}$, $D_{(2,5)}(p) = 0$ otherwise. The formulas in Table 2.1 follow and the proof is complete. □

As a simple consequence of Table 2.1, one sees that the number of primes satisfying $R^d_{(1,b,c)}(p) = m$, $m \geq 0$, are determined by specific values of the class number of binary quadratic forms with negative fundamental discriminants.

Corollary 2.1. *Let $m \geq 0$ be a fixed positive integer. For the fifteen ternary quadratic forms in Table 2.1, the number of primes satisfying $R^d_{(1,b,c)}(p) = m$ is determined by Table 2.2 in case $m = 0$ and by Table 2.3 in case $m \geq 1$. In particular, for fixed $m \geq 1$, there are only a finite number of primes with the stated conditions.*

Proof. This follows from Theorem 2.2. If $m \geq 1$ one notes that there are only a finite number of discriminants D with given class number $h(D)$, as already shown by Gauss [14]. □

The class number formulas in the Table 2.3 imply some interesting congruence conditions.

Table 2.3
Class number conditions for solving the equation $R^d_{(1,b,c)}(p) = m \geq 1$.

Form	Arithmetic progression	Condition	Form	Arithmetic progression	Condition
$(1,1,1)$	$p \equiv 1\ (8)$	$h(-4p) = 4m$	$(1,4,4)$	$p \equiv 1,9\ (40)$	$h(-4p) = 4m-4$
	$p \equiv 5\ (8)$	$h(-4p) = 4m+2$			$m \geq 2$
	$p \equiv 3\ (8)$	$h(-p) = 2m-1$		$p \equiv 17,25,33\ (40)$	$h(-4p) = 4m$
				$p \equiv 21,29\ (40)$	$h(-4p) = 4m-2$
$(1,1,2)$ & $(1,2,4)$	$p \equiv 1\ (8)$	$h(-8p) = 4m+4$	$(1,8,8)$	$p \equiv 1\ (8)$	$h(-4p) = 4m-4$
	$p \equiv 3,5\ (8)$	$h(-8p) = 4m+2$			$m \geq 2$
	$p \equiv 7\ (8)$	$h(-8p) = 4m$			
$(1,1,4)$	$p \equiv 1(4)$	$h(-4p) = 2m+2$	$(1,2,16)$	$p \equiv 1\ (8)$	$h(-8p) = 4m+4$
				$p \equiv 3\ (8)$	$h(-8p) = 4m+2$
$(1,1,8)$ & $(1,4,8)$	$p \equiv 1\ (8)$	$h(-8p) = 4m+4$	$(1,8,16)$	$p \equiv 1\ (8)$	$h(-8p) = 4m+4$
	$p \equiv 5\ (8)$	$h(-8p) = 4m+2$			
$(1,2,8)$	$p \equiv 1\ (8)$	$h(-4p) = 2m+2$	$(1,1,3)$	$p \equiv 1\ (24)$	$h(-3p) = 4k$,
	$p \equiv 3\ (8)$	$h(-p) = 2k+1$,			$m = 3k-1$
		$m = 3k+1$		$p \equiv 17\ (24)$	$h(-3p) = 4k-2$,
$(1,2,2)$	$p \equiv 1\ (8)$	$h(-4p) = 4m$			$m = 3k-2$
	$p \equiv 5\ (24)$	$h(-4p) = 4m-6$		$p \equiv 5\ (24)$	$h(-3p) = 2m$
		$m \geq 2$		$p \equiv 13\ (24)$	$h(-3p) = 2m+2$
	$p \equiv 13,21\ (24)$	$h(-4p) = 4m-2$		$p \equiv 7,19\ (24)$	$h(-12p) = 8m+4$
	$p \equiv 11\ (24)$	$h(-p) = 2k+1$		$p \equiv 11\ (24)$	$h(-12p) = 8m-4$
		$m = 3k+2$		$p \equiv 23\ (24)$	$h(-12p) = 8m$
	$p \equiv 3,19\ (24)$	$h(-p) = 2k+1$			
		$m = 3k+1$			
$(1,2,3)$	$p \equiv 1,11,19\ (24)$	$h(-24p) = 8m+8$	$(1,1,5)$	$p \equiv 1,9\ (20)$	$h(-20p) = 8m+8$
	$p \equiv 5,7,13,17\ (24)$	$h(-24p) = 8m+4$		$p \equiv 17,33\ (40)$	$h(-20p) = 8m+4$
	$p \equiv 23\ (24)$	$h(-24p) = 8m$		$p \equiv 13,37\ (40)$	$h(-20p) = 8m$
				$p \equiv 31,39\ (40)$	$h(-5p) = 4m$
				$p \equiv 7,23\ (40)$	$h(-5p) = 4m-2$

Corollary 2.2. *Let p be an odd prime number. Then, the class numbers of the fundamental discriminants $D = -kp$, $k \in \{3,4,5,8,12,20,24\}$ satisfy the following necessary congruence properties:*

$$\text{(P1)} \quad \begin{cases} p \equiv 1 \pmod 8 & \Rightarrow \quad h(-4p) \equiv 0 \pmod 4, \\ p \equiv 5 \pmod 8 & \Rightarrow \quad h(-4p) \equiv 2 \pmod 4. \end{cases}$$

$$\text{(P2)} \quad \begin{cases} p \equiv 1,7 \pmod 8 & \Rightarrow \quad h(-8p) \equiv 0 \pmod 4, \\ p \equiv 3,5 \pmod 8 & \Rightarrow \quad h(-8p) \equiv 2 \pmod 4. \end{cases}$$

$$\text{(P3)} \quad \begin{cases} p \equiv 1 \pmod{24} & \Rightarrow \quad h(-3p) \equiv 0 \pmod 4, \\ p \equiv 17 \pmod{24} & \Rightarrow \quad h(-3p) \equiv 2 \pmod 4, \\ p \equiv 5,13 \pmod{24} & \Rightarrow \quad h(-3p) \equiv 0 \pmod 2. \end{cases}$$

$$\text{(P4)} \quad \begin{cases} p \equiv 23 \pmod{24} & \Rightarrow \quad h(-12p) \equiv 0 \pmod 8, \\ p \equiv 7, 11, 19 \pmod{24} & \Rightarrow \quad h(-12p) \equiv 4 \pmod 8. \end{cases}$$

$$\text{(P5)} \quad \begin{cases} p \equiv 1, 11, 19, 23 \pmod{24} & \Rightarrow \quad h(-24p) \equiv 0 \pmod 8, \\ p \equiv 5, 7, 13, 17 \pmod{24} & \Rightarrow \quad h(-8p) \equiv 4 \pmod 8. \end{cases}$$

$$\text{(P6)} \quad \begin{cases} p \equiv 7, 23 \pmod{40} & \Rightarrow \quad h(-5p) \equiv 2 \pmod 4, \\ p \equiv 31, 39 \pmod{40} & \Rightarrow \quad h(-5p) \equiv 0 \pmod 4. \end{cases}$$

$$\text{(P7)} \quad \begin{cases} p \equiv 1, 9 \pmod{20} \vee p \equiv 13, 37 \pmod{40} & \Rightarrow \quad h(-20p) \equiv 0 \pmod 8, \\ p \equiv 17, 33 \pmod{40} & \Rightarrow \quad h(-20p) \equiv 4 \pmod 8. \end{cases}$$

Proof. The formulas in Table 2.3 imply these results as follows: $(1,1,1) \Rightarrow$ (P1), $(1,1,2) \Rightarrow$ (P2), $(1,1,3) \Rightarrow$ (P3) and (P4), $(1,2,3) \Rightarrow$ (P5), $(1,1,5) \Rightarrow$ (P6) and (P7). □

Remarks 2.1. It is important to observe that the congruence properties (P1)–(P7) are known, some for a long time. Improvements are possible and have consequences on solving the equation $R^d_{(1,b,c)}(p) = m \geq 1$, as shown below. According to Brink [5] the property (P1) even characterizes the primes $p \equiv 1 \pmod 4$, a result already derived by Glaisher [15] (see also Lerch [25], p. 224). Glaisher also characterizes the set of all odd primes by the property (P2). A unified approach to the congruences (P1)–(P7) with some improvements and further references is found in Berndt [4]. For still further information consult the monograph by Urbanowicz and Williams [34], Chap. II. Divisibility properties by higher powers of 2 depend upon the 2-Sylow subgroup structure of the class group, which has often been studied (e.g. Rédei [28], Shanks [30], Dominguez et al. [13], etc.). Some comments on the use of (P1)–(P7) and its improvements should be useful. With them, some statements in Table 2.3 can be strengthened. For example, with (P1), the condition in Table 2.3 for the form $(1,1,4)$ can be improved to the more precise condition:

$$\begin{aligned} &h(-4p) = 2m+2, \ m \text{ odd}, \ p \equiv 1 \pmod 8, \\ &h(-4p) = 2m+2, \ m \text{ even}, \ p \equiv 5 \pmod 8. \end{aligned} \tag{2.8}$$

As already said, in some cases the properties (P1)–(P7) are not best possible. For example, instead of (P3), Corollary 4.4 in Berndt [4] states the more stringent property:

$$\text{(P3}') \quad \begin{cases} p \equiv 1 \pmod{12} & \Rightarrow \quad h(-3p) \equiv 0 \pmod 4, \\ p \equiv 5 \pmod{12} & \Rightarrow \quad h(-3p) \equiv 2 \pmod 4. \end{cases}$$

With this, solving $R^d_{(1,1,3)}(p) = m \geq 1$ for the primes $p \equiv 5, 13 \pmod{24}$ can be made more precise. For $p \equiv 5 \pmod{24}$, respectively $p \equiv 13 \pmod{24}$, the condition $h(-3p) = 2m$, respectively $h(-3p) = 2m+2$, is only possible for odd m. Similarly, using Corollary 5.4 in Berndt [4], the property (P6) can be improved to

$$(\mathrm{P6}') \qquad \begin{cases} p \equiv 7, 23 \pmod{40} & \Rightarrow \quad h(-5p) \equiv 2 \pmod 4, \\ p \equiv 31 \pmod{40} & \Rightarrow \quad h(-5p) \equiv 4 \pmod 8, \\ p \equiv 39 \pmod{40} & \Rightarrow \quad h(-5p) \equiv 0 \pmod 8. \end{cases}$$

With this, the condition $h(-5p) = 4m$ for the form $(1, 1, 5)$ in Table 2.3 is only possible for odd m if $p \equiv 31 \pmod{40}$ and even m if $p \equiv 39 \pmod{40}$.

3. Universal zero-free property, infinite and finite exceptional sets

We present the detailed analysis of the universal zero-free property (Definitions 1.1) and a description of the infinite and finite exceptional sets (Definitions 1.2) for the fifteen ternary quadratic forms $(1, b, c)$ listed in Theorem 2.1. Based on Corollary 2.1, Table 2.2, one sees that the structure of the solutions to $R^d_{(1,b,c)}(p) = 0$ depends upon the imaginary quadratic fields with even discriminant two and four, which have been completely determined by Stark [31] and Arno [1] respectively. Recall the following notion (e.g. Cohen [6], Definition 5.1.2).

Definition 3.1. An integer D is called a *fundamental discriminant* if D is the discriminant of a quadratic field. This means that $D \neq 1$ and either $D \equiv 1 \pmod 4$ is squarefree, or $D \equiv 0 \pmod 4$, $D/4$ is squarefree and $D/4 \equiv 2, 3 \pmod 4$.

Theorem 3.1. *Based on Definitions 1.1 and 1.2, the fifteen ternary quadratic forms* $(1, b, c)$ *from Table 2.1 are completely classified by the Table 3.1.*

Proof. The discriminants of relevance $D = -kp$, $k \in \{1, 3, 4, 5, 8, 12, 20, 24\}$ are all fundamental discriminants by Definition 3.1. Using the two sets of negative fundamental discriminants with class numbers two and four (e.g. Weisstein [37]), it is straightforward to filter out all primes $p \geq 1 + b + c$ that satisfy the required class number conditions for finite exceptional sets. The remaining assertions are consequences of the results stated in the Tables 2.2 and 2.3. □

Some comments are in order. The only Bell forms with empty finite exceptional sets are the forms $(1, 2, 2)$, $(1, 2, 8)$, $(1, 4, 4)$ and $(1, 8, 8)$. The only forms, which do not satisfy the universal zero-free property for some arithmetic progression of primes are the forms $(1, 1, 8)$, $(1, 4, 8)$, and $(1, 8, 16)$. The strictly universal zero-free forms $(1, 1, 2)$, $(1, 1, 3)$, $(1, 2, 3)$ and $(1, 2, 4)$ have been previously discussed in the introductory Section 1. By the Definitions 1.1 and 1.2, if a form is not strictly universal, then the union of the residue classes within the sets $P(r, m)$ and $F(r, m)$ in the three columns of Table 3.1 always encompass the whole set of odd primes. Except for the form $(1, 1, 5)$ (residue classes mod 40) these are the residue classes mod 8.

Table 3.1
Universal zero-free forms, infinite and finite exceptional sets for selected forms.

Form	Universal zero-free sets	Infinite exceptional sets	Finite exceptional sets
$(1,1,1)$	$P(r,8)$, $r=1,3$	$P(7,8)$	$F(5,8)=\{5,13,37\}$
$(1,1,2)$	strictly universal	none	$F(1,8)=\{17,41\}$, $F(3,8)=\{11\}$, $F(5,8)=\{5,29\}$
$(1,1,4)$	$P(1,8)$	$P(r,8)$, $r=3,7$	$F(5,8)=\{13,37\}$
$(1,1,8)$	none	$P(r,8)$, $r=3,7$	$F(1,8)=\{17,41\}$, $F(5,8)=\{29\}$
$(1,2,2)$	$P(r,8)$, $r=1,3,5$	$P(7,8)$	none
$(1,2,4)$	strictly universal	none	$F(1,8)=\{17,41\}$, $F(3,8)=\{11\}$, $F(5,8)=\{29\}$
$(1,2,8)$	$P(r,8)$, $r=1,3$	$P(r,8)$, $r=5,7$	none
$(1,4,4)$	$P(r,8)$, $r=1,5$	$P(r,8)$, $r=3,7$	none
$(1,4,8)$	none	$P(r,8)$, $r=3,7$	$F(1,8)=\{17,41\}$, $F(5,8)=\{29\}$
$(1,8,8)$	$P(1,8)$	$P(r,8)$, $r=3,5,7$	none
$(1,2,16)$	$P(3,8)$	$P(r,8)$, $r=5,7$	$F(1,8)=\{41\}$
$(1,8,16)$	none	$P(r,8)$, $r=3,5,7$	$F(1,8)=\{41\}$
$(1,1,3)$	strictly universal	none	$F(7,24)=\{7,31\}$, $F(19,24)=\{19\}$
$(1,2,3)$	strictly universal	none	$F(1,24)=\{73\}$, $F(11,24)=\{11,83\}$, $F(19,24)=\{19,43\}$, $F(7,24)=\{7\}$, $F(13,24)=\{13\}$, $F(17,24)=\{17\}$
$(1,1,5)$	$P(r,40)$, $r=7,13,23,31,33,37,39$	$P(3,8)$	$F(1,40)=\{41\}$, $F(21,40)=\{101\}$, $F(9,40)=\{89\}$, $F(29,40)=\{29\}$, $F(17,40)=\{17\}$

4. Zero-free prime representations by ternary quadratic forms in essentially m ways

From a historical perspective, the present topic is related to the problem of expressing a positive integer as a sum of three squares in essentially one way studied first by Bateman and Grosswald [2], and completely solved by Arno [1] (see also Grosswald [16], Chapter 7, Theorem 4). The original version of the problem, which goes back to Lehmer [24], asks for the number of partitions of a positive integer n as a sum of three squares, denoted by $P_3(n)$, i.e., the number of integer triples (x,y,z) solving the equation $n=x^2+y^2+z^2$, $0\leq x\leq y\leq z$. Bateman and Grosswald [2] asked for all n satisfying $P_3(n)=1$. If $n\equiv 3 \pmod 8$ the solution is a simple consequence of the determination of the imaginary quadratic fields with odd discriminant and class number one or two. In this case, one finds twelve solutions, namely

$$P_3(n)=1 \quad \Leftrightarrow \quad n\in\{3,11,19,35,43,67,91,115,163,235,403,427\}. \tag{4.1}$$

For the primes $p\equiv 3 \pmod 8$ among them, which all have class number one, one finds the six solutions

$$R_3^d(p)=1 \quad \Leftrightarrow \quad P_3(p)=1 \quad \Leftrightarrow \quad p\in\{3,11,19,43,67,163\}. \tag{4.2}$$

The first equivalence holds because a sum of three squares is congruent to 3 mod 8 if, and only if, all three squares are odd. If $n\equiv 1,2,5,6 \pmod 8$ the solution depends upon the knowledge of all the imaginary quadratic fields with even discriminant and

Table 4.1
The number of primes (not congruent to 7 mod 8) satisfying $R_3^d(p) = m$, $m \leq 5$.

m	$\#\{p : R_3^d(p) = m\}$	$p \equiv 3 \pmod 8$	$p \equiv 1 \pmod 8$	$p \equiv 5 \pmod 8$
0	3	0	0	3
1	17	6	4	7
2	35	14	7	14
3	43	21	10	12
4	51	26	11	14
5	56	29	16	11

class number one, two or four. The thirty-three fields with this property give rise to twenty-one integers n satisfying

$$P_3(n) = 1 \quad \Leftrightarrow$$
$$n \in \{1, 2, 5, 6, 10, 13, 14, 21, 22, 30, 37, 42, 46, 58, 70, 78, 93, 133, 142, 190, 253\}. \quad (4.3)$$

Unfortunately, none of the prime solutions are expressible without zero squares components, and (4.3) do not lead to any solution of $R_3^d(p) = 1$. In fact, the structure of the solutions to $R_3^d(p) = 1$ differs completely when $p \equiv 1, 5 \pmod 8$ and depends via Corollary 2.1 upon the imaginary quadratic fields with even discriminant four and six, where the last ones have been completely determined by Wagner [35]. In this case, one finds the eleven primes

$$R_3^d(p) = 1 \quad \Leftrightarrow \quad p \in \{17, 29, 53, 61, 73, 97, 109, 157, 193, 277, 397\}. \quad (4.4)$$

Therefore, one has a total of seventeen primes satisfying the condition $R_3^d(p) = 1$.

The problem of determining the number of primes and the primes satisfying the equation $R_{(1,b,c)}^d(p) = m$ for our fifteen ternary quadratic forms can be solved similarly. In general, to find all primes satisfying $R_{(1,b,c)}^d(p) = m$, $m \geq 0$, one uses Corollary 2.1 and modern computations of the class number of imaginary quadratic fields with arbitrary discriminants. Note that Watkins [36], Table 4, provides for each $N \leq 100$ the number of negative fundamental discriminants with class number N and the largest such discriminant in absolute value. Especially useful are the lists of negative fundamental discriminants with class number $N \leq 25$ by Weisstein [37]. Beyond this it might be necessary to apply some more sophisticated computational methods (e.g. Cohen [6], Sections 5.3 and 5.4, Mosunov and Jacobson [26]). Analytical methods to challenge these properties are also of interest. On the other hand, in analogy to the well-known Taxicab numbers, one might consider the smallest, respectively largest, prime in a given arithmetic progression $p \equiv r \pmod s$, denoted by $S_{(1,b,c)}(m, r, s)$ respectively $L_{(1,b,c)}(m, r, s)$, that is expressible by a ternary quadratic form $(1, b, c)$ with three non-zero squares in essentially m ways. The finite number of such primes, denoted by $N_{(1,b,c)}(m, r, s)$, might also be of interest. To illustrate, only sums of three squares are considered. For $m \leq 5$ the numbers of primes $N_{(1,1,1)}(m, r, s)$ are listed in the Table 4.1. The numbers $S_{(1,1,1)}(m, r, s)$ and $L_{(1,1,1)}(m, r, s)$ are found in Table 4.2.

Table 4.2
The primes $S_{(1,1,1)}(m,r,s)$ and $L_{(1,1,1)}(m,r,s)$ (in parentheses) for $1 \leq m \leq 5$.

m	$p \equiv 3$ (8)	$p \equiv 1$ (8)	$p \equiv 5$ (8)
1	3 (163)	17 (193)	29 (397)
2	59 (907)	41 (577)	181 (1213)
3	131 (2683)	89 (2017)	107 (2293)
4	251 (5923)	257 (3217)	293 (3733)
5	419 (10627)	281 (4153)	269 (6637)

Conflict of interest statement

The author declares that his has no financial and non-financial competing interests.

Acknowledgment

The author is grateful to a referee for his comments and suggestions for clarification and improvements.

References

[1] S. Arno, The imaginary quadratic fields of class number 4, Acta Arith. 60 (1992) 321–334.
[2] P.T. Bateman, E. Grosswald, Positive integers expressible as a sum of three squares in essentially only one way, J. Number Theory 19 (1984) 301–308.
[3] E.T. Bell, The numbers of representations of integers in certain forms $ax^2 + by^2 + cz^2$, Amer. Math. Monthly 31 (3) (1924) 126–131.
[4] B.C. Berndt, Classical theorems on quadratic residues, Enseign. Math. 22 (1976) 261–304.
[5] D. Brink, Two theorems of Glaisher and Kaplansky, Funct. Approx. Comment. Math. 41 (2) (2009) 163–165.
[6] H. Cohen, A Course in Computational Algebraic Number Theory, Grad. Texts in Math., vol. 138, Springer-Verlag, Berlin, Heidelberg, 1993.
[7] S. Cooper, M.D. Hirschhorn, On the number of primitive representations of integers as sums of squares, Ramanujan J. 13 (2007) 7–25.
[8] D.A. Cox, Primes of the form x^2+ny^2, in: Fermat, Class Field Theory, and Complex Multiplication, 2nd ed., John Wiley & Sons, Hoboken, New Jersey, 2013.
[9] L.E. Dickson, History of the Theory of Numbers, vol. II, Carnegie Institute of Washington, Washington, 1920, reprint: Chelsea, New York, 1966.
[10] L.E. Dickson, Integers represented by positive ternary quadratic forms, Bull. Amer. Math. Soc. 33 (1927) 63–70.
[11] L.E. Dickson, Introduction to the Theory of Numbers, University of Chicago Press, 1929, reprint: Dover Publications, 1957.
[12] P.G.L. Dirichlet, Über die Zerlegbarkeit der Zahlen in drei Quadrate, J. Reine Angew. Math. 40 (1850) 228–232 (Werke, vol. 2, Springer, Berlin, 1897, pp. 89–96. Reprint: Chelsea, 1969).
[13] C. Dominguez, S.J. Miller, S. Wong, Quadratic fields with cyclic 2-class groups, J. Number Theory 133 (2013) 926–939.
[14] C.F. Gauss, Disquitiones Arithmeticae, Fleischer, Leipzig, 1801, German translation: Untersuchungen über höhere Arithmetik, Springer, 1889. Reprint: Chelsea, 1965. English translation: Yale, 1966; Springer, 1986.
[15] J.W.L. Glaisher, On the expressions for the number of classes of a negative determinant, and on the numbers of positives in the octants of P, Quart. J. Pure App. Math. 34 (1903) 178–204.
[16] E. Grosswald, Representations of Integers as Sums of Squares, Springer, New York, 1985.
[17] X. Guo, Y. Peng, H. Qin, On the representation numbers of ternary quadratic forms and modular forms of weight 3/2, J. Number Theory 140 (2014) 235–266.

[18] W. Hürlimann, Exact and asymptotic evaluation of the number of distinct primitive cuboids, J. Integer Seq. 18 (2) (2015) 15.2.5.
[19] W. Hürlimann, On the number of primitive Pythagorean quintuples, J. Algebra Number Theory Adv. Appl. 13 (1) (2015) 13–28.
[20] W. Hürlimann, Cooper and Lam's conjecture for generalized Bell ternary quadratic forms, J. Number Theory 158 (2016) 23–32.
[21] W. Hürlimann, Eperson's conjecture on sums of three squares: short proof of an improved result, Int. Math. Forum 11 (2) (2016) 95–100.
[22] W. Hürlimann, Zero-free primitive square representations by some ternary quadratic forms, J. Algebra Number Theory Adv. Appl. 15 (1) (2016) 77–100.
[23] I. Kaplansky, Ternary positive quadratic forms that represent all odd positive integers, Acta Arith. 70 (1995) 209–214.
[24] D.H. Lehmer, On the partition of numbers into squares, Amer. Math. Monthly 55 (1948) 476–481.
[25] M. Lerch, Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers, Acta Math. 30 (1906) 203–293.
[26] A.S. Mosunov, M.J. Jacobson Jr., Unconditional class group tabulation of imaginary quadratic fields to $|\Delta| < 2^{40}$, Math. Comp. (2015), http://dx.doi.org/10.1090/mcom3050 (early view).
[27] L. Panaitopol, On the representation of natural numbers as sum of squares, Amer. Math. Monthly 112 (2005) 168–171.
[28] L. Rédei, Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung, Acta Math. Acad. Sci. Hungar. 4 (1953) 31–87.
[29] H.P. Rehm, On a theorem of Gausz concerning the number of integral solutions of the equation $x^2 + y^2 + z^2 = m$, in: O. Taussky (Ed.), Ternary Quadratic Forms and Norms, in: Lect. Notes Pure Appl. Math., vol. 79, Marcel Dekker, New York and Basel, 1982, pp. 31–38.
[30] D. Shanks, Gauss's ternary form reduction and the 2-Sylow subgroup, Math. Comp. 25 (1971) 837–853. Corrigenda: Math. Comp. 32 (1978) 1328–1329.
[31] H.M. Stark, On complex quadratic fields with class number two, Math. Comp. 29 (1975) 289–302.
[32] Z.H. Sun, My conjectures in number theory, last modified March 29, 2007, preprint, http://www.hytc.edu.cn/xsjl/szh/mycon.pdf, 2007.
[33] Z.H. Sun, K.S. Williams, On the number of representations of n by $ax^2 + bxy + cy^2$, Acta Arith. 122 (2) (2006) 101–171.
[34] J. Urbanowicz, K.S. Williams, Congruences for L-Functions, Math. Appl., vol. 511, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2000.
[35] C. Wagner, Class number 5, 6 and 7, Math. Comp. 65 (1996) 785–800.
[36] M. Watkins, Class numbers of imaginary quadratic fields, Math. Comp. 73 (2004) 907–938.
[37] E.W. Weisstein, Class number, from MathWorld – a Wolfram Web Resource, http://mathworld.wolfram.com/ClassNumber.html, 1999–2015.
[38] K.S. Williams, Ternary quadratic forms $ax^2 + by^2 + cz^2$ representing all positive integers $8k + 4$, Acta Arith. 166 (4) (2014) 391–396.
[39] K.S. Williams, A "four integers" theorem and a "five integers" theorem, Amer. Math. Monthly 122 (6) (2015) 528–536.