Shirali's Questions About Sums of Residues of Squares

John P. Robertson
Boonton, NJ

Shirali's article [16] gives a delightful account of some of the differences between primes of the forms $4k+1$ and $4k+3$. In doing so he raises questions about the relation between certain sums of residues of squares and those integers $d > 0$ for which the ring of integers of the field $\mathbb{Q}\left(\sqrt{-d}\right)$ has the unique factorization property. We will show that a recent theorem of Schinzel can be used to answer the questions Shirali raises and to extend some results that Shirali presents. Along the way, we give a brief introduction to class numbers of negative discriminants.

Shirali [16, pp. 266–268] proves the following surprising theorem (for another proof see [13, pp. 113, 304–305]). In this article, $\lfloor x \rfloor$ denotes the greatest integer not exceeding x, $\lceil x \rceil$ denotes the least integer greater than or equal to x, and $\{x\}$ denotes the fractional part of x, i.e., $\{x\} = x - \lfloor x \rfloor$.

THEOREM 1. *If p is a prime number of the form $4k+1$, then*

$$\sum_{i=1}^{\lfloor p/4 \rfloor} \left\lfloor \sqrt{ip} \right\rfloor = \frac{p^2-1}{12}.$$

Shirali's proof involves certain sums of residues of squares. Namely, define $\mathrm{Rem}(i^2 \div n)$ to be the least nonnegative residue of i^2 modulo n, i.e., $\mathrm{Rem}(i^2 \div n) = n\,\{i^2 \div n\}$. Shirali considers the sum[1] $R(n) = \sum_{i=1}^{n-1} \mathrm{Rem}(i^2 \div n)$, and shows that if n is a product of distinct primes of the form $4k+1$ then $R(n)/2n = (n-1)/4 = \lfloor n/4 \rfloor$. More generally, he shows that if n is a

[1] Actually, Shirali defines $R(n)$ only for odd n, and here we extend the definition to include even n. Also, he takes the sum to $(n-1)/2$, so, for odd n, our sum is double his sum.

product of primes of the form $4k+1$, possibly repeated, and if a is the largest integer so that a^2 divides n, then $R(n)/2n = (n-a)/4$.

His observations lead to questions about the sum $R(n)$ for other n. One question Shirali investigates is, for what odd n, other than those above, is $R(n)/2n = \lfloor n/4 \rfloor$? Empirically he found that the only other odd n less than 10^5 for which this holds are 7, 11, 19, 43, 67, and 163. He notes that [16, p. 270], "these numbers are part of a *very* famous list — the integers $d > 0$ for which the ring of integers of the field $\mathbb{Q}\left(\sqrt{-d}\right)$ has the unique factorization property." The only other numbers in this last list are 1, 2, and 3. He states [16, p. 270], "It remains unclear whether there is any immediate connection between the property being studied in this section and that of unique factorization, or whether we have at hand a rather fantastic coincidence."

Shirali shows that if n is of the form $25b$ where b is a product of distinct primes of the form $4k+1$, then $(n-1)/4 - R(n)/2n = 1$. He observes, based on empirical evidence, that this last equation also holds for $n = 77, 133, 209, \ldots, 10921$. Each of the numbers in this last list is the product of exactly two distinct numbers from the list (above) 7, 11, 19, 43, 67, 163. He finds that this does not seem to hold for products of four primes from this list, and states [16, p. 270], "The pattern is rather obscure at this stage."

We will answer the questions he raises, extend Theorem 1, and discuss the converse of Theorem 1.

Class numbers

A recent theorem of Schinzel that we will make great use of below involves *class numbers*, so this section gives some background. Readers familiar with class numbers can safely skip this section.

One way that class numbers arise is in the study of binary quadratic forms $f = f(x, y) = ax^2 + bxy + cy^2 = (a, b, c)$. Investigations of which integers m could be represented by which forms (a, b, c), i.e., for which forms

is there a pair of integers $(x,\, y)$ so that $ax^2 + bxy + cy^2 = m$, led to notions of equivalence classes of forms. Two forms f and g are *equivalent* if there is an integer matrix $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ so that $\det(A) = \pm 1$ and $g(x,\, y) = f(\alpha x + \beta y,\, \gamma x + \delta y)$, and they are *properly equivalent* if this determinant is $+1$. It is easy to see that equivalence and proper equivalence establish equivalence relations among forms.

Two forms that are equivalent will represent the same m's. If $(a,\, b,\, c)$ is equivalent to $(a',\, b',\, c')$ then $b^2 - 4ac = b'^2 - 4a'c'$. The value $b^2 - 4ac$ is called the *discriminant* of the form $(a,\, b,\, c)$. We consider only those forms whose discriminant is not a square; these are the forms that do not factor into linear terms in x and y. In particular, for the forms of interest, $ac \neq 0$. A form is *primitive* if $\gcd(a,\, b,\, c) = 1$. Within a given equivalence class, either all forms are primitive, or none are.

Because, for the forms of interest, $a \neq 0$, we have that $ax^2 + bxy + cy^2 = [(2ax + by)^2 - Dy^2]/(4a)$. If $D < 0$ the form represents only positive values or represents only negative values depending on whether a is positive or negative. For the remainder of this article, we will only be concerned only with *positive definite* forms, i.e., those with $D < 0$ and $a > 0$. For discriminants $D > 0$ see [5, 7, 14].

Of all forms with a given discriminant $D < 0$, the number of proper equivalence classes of (positive definite) primitive forms is called the *class number* of D, written $h(D)$ [5, p. 226] [9, p. 29]. Within each proper equivalence class of quadratic forms there is a unique form that is *reduced*, i.e., a form $(a,\, b,\, c)$ for which $|b| \leq a \leq c$ and if $|b| = a$ or $a = c$ then $b \geq 0$. The class number can be computed by just counting the number of reduced primitive forms [5, pp. 226–229] [9, p. 29].

As an example, let's compute the class number of the discriminant -20. The following conditions on reduced forms are easy to see [14, p. 124] [5, p. 227]: $|b| \leq a \leq \sqrt{|D|\,/3}$, $b^2 \equiv D \pmod 4$, a divides $(b^2 - D)/4$, and $a \leq (b^2 - D)/4a = c$. (For the first note that $|D| = 4ac - b^2 \geq 4a^2 - a^2$, so

$a^2 \leq |D|/3$.) For $D = -20$, we need only check those cases with $|b| \leq \sqrt{20/3}$ or $|b| \leq 2$. For 4 to divide $b^2 - D = b^2 + 20$, b has to be even, so we need only try $b = -2$, 0, and 2. For $b = \pm 2$, $(b^2 - D)/4 = 6$, so $a \geq 2 = |b|$, a divides 6, and $a \leq 6/a$. Only $a = 2$ meets all these criteria. For there to be a reduced form with $a = 2$ and $|b| = 2$, b must be $+2$, and c is 3. The form $(2, 2, 3)$ is then the only reduced form with $|b| = 2$. For $b = 0$, $(b^2 - D)/4 = 5$, so $a > 0$ divides 5, and $a \leq 5/a$. The only such a is $a = 1$, giving $c = 5$, and $(1, 0, 5)$ as the only reduced form with $b = 0$. Thus the discriminant -20 has two primitive reduced forms, (1, 0, 5) and (2, 2, 3), and $h(-20) = 2$.

The equations $|b| \leq a \leq \sqrt{|D|/3}$, $c = (b^2 - D)/4a$ imply that the number of reduced forms, for a given negative discriminant D, is finite. Any nonsquare integer D (positive or negative) congruent to 0 or 1 modulo 4 is the discriminant of some binary quadratic form. If $D \equiv 0 \pmod 4$, the form $x^2 - (D/4)y^2$ has discriminant D. If $D \equiv 1 \pmod 4$, the form $x^2 + xy - ((D-1)/4)y^2$ has discriminant D. In particular, this shows that, for $D < 0$, $h(D)$ is a positive integer. (For $D > 0$, $h(D)$ is also defined, and is also a positive integer.)

For a given integer $s > 0$, there are only finitely many negative discriminants $-D$, with $D > 0$, that have class number $h(-D)$ equal to s [14, p. 159] [5, p. 290] [9, pp. 149, 158]. In particular, it has been proved that the only $D > 0$ so that $h(-D) = 1$ are 3, 4, 7, 8, 11, 12, 16, 19, 27, 28, 43, 67, 163 [9, p. 149]. You will observe that this list has many entries in common with a list in the opening section. This one is slightly different in that this is a list of discriminants, while that in the opening section is a list of $|d|$ where $d < 0$ is squarefree and the quadratic field $\mathbb{Q}(\sqrt{d})$ has unique factorization. But, the two lists are equivalent for the reasons we now outline.

For squarefree d, the field $\mathbb{Q}(\sqrt{d})$ has a discriminant D, defined as $D = d$ if $d \equiv 1 \pmod 4$, and $D = 4d$ otherwise. There is a correspondence between the field $\mathbb{Q}(\sqrt{d})$ with discriminant D and the set of binary quadratic forms with discriminant D. The field $\mathbb{Q}(\sqrt{d})$ has unique factorization if and only if $h(D)$, as defined above in terms of binary quadratic forms, is 1. Those

squarefree $d < 0$ so that $\mathbb{Q}(\sqrt{d})$ has unique factorization are $d = -1$, -2, -3, -7, -11, -19, -43, -67, and -163, and the discriminants of these fields are -4, -8, -3, -7, -11, -19, -43, -67, -163 respectively. This accounts for nine of the 13 negative discriminants that have class number 1. This leaves the discriminants -12, -16, -27, and -28, which also have class number 1. These are the discriminants of *orders*, which are certain subrings of the ring of integers of $\mathbb{Q}(\sqrt{d})$ for $d = -3$, -2, -3, -7 respectively. It would take us too far afield to cover this in any detail, but for more on the connection between quadratic forms and quadratic fields $\mathbb{Q}(\sqrt{d})$ (and their orders) see [5, pp. 218–225] [7, pp. 138–143] [8, pp. 200–207] [9, pp. 113, 132–142, 153–156] [14, pp. 146–153]. For more on the connection between class number 1 and unique factorization see any of these last five references, or [17, Chapter 9].

There is a table of class numbers of $\mathbb{Q}(\sqrt{d})$ in [17, p. 197] for $|d| < 100$, d squarefree and not a square. The (free) computer package PARI [6] has a routine, qfbclassno(x), to compute class numbers of discriminants. Cohen [5, pp. 228–256] gives several routines to compute class numbers, including one that implements the above method of counting reduced forms. For large discriminants, the more sophisticated methods given in [5] are useful.

Appendix A lists all D so that $-D$ is a discriminant with class number 1, 2, or 3. For the fascinating history of the determination of all negative discriminants with class number up to 3, see [10]. For more on this and for higher class numbers, see [1, 2, 11, 12, 18].

Schinzel's theorem

A direct corollary of a remarkable theorem recently proved by Schinzel [15] will allow us to address Shirali's questions and observations. Schinzel's full theorem is given in Appendix B. The corollary is

THEOREM 2 [SCHINZEL, 2001]. *If n is a positive integer, and a (or $a(n)$) is the largest integer so that a^2 divides n, then*

$$\frac{n-a}{2} - \frac{R(n)}{n} = \sum_{\substack{r>0,\ r|n \\ r \equiv 0 \text{ or } 3 \ (\bmod 4)}} e_r h(-r),$$

where $R(n)$ is the sum defined following Theorem 1; e_r is $1/3$ if $r = 3$, $1/2$ if $r = 4$, and 1 otherwise; and $h(-r)$ is the class number of the discriminant $-r$.

For example, if $n = 12$ then $a = 2$, $R(12) = 1+4+9+4+1+0+1+4+9+4+1 = 38$, and the right-hand-side sum is $e_3h(-3) + e_4h(-4) + e_{12}h(-12) = (1/3)(1) + (1/2)(1) + (1)(1) = 11/6$. Sure enough, $(12-2)/2 - 38/12 = 11/6$.

Readers familiar with the Dirichlet analytic class number formula [3, p. 344] [4, p. 16] will recognize that both Theorem 2 and the Dirichlet class number formula relate class numbers to sums involving residues of squares.

For notational convenience, let S (or $S(n)$) denote the sum on the right hand side of the equation in Theorem 2. Observe that $S \geq 0$ and that $S = 0$ only if n is not divisible by 4 or by any prime of the form $4k + 3$. If 3 or 4, or both, divide n then S is not an integer, while if neither 3 nor 4 divides n, then S is an integer. Without further ado, let us use Theorem 2 to address Shirali's questions.

Solutions to $\lfloor n/4 \rfloor = R(n)/(2n)$

Shirali looked for odd n so that $\lfloor n/4 \rfloor = R(n)/(2n)$. He showed this holds for n a squarefree product of primes of the form $4k + 1$, and for $n = 7$, 11, 19, 43, 67, and 163. We will use Theorem 2 to show that these are the only solutions to this equation among all positive integers, odd or even.

Separate cases according to congruence classes of n modulo 4. First, consider $n \equiv 1 \ (\bmod\ 4)$, so $\lfloor n/4 \rfloor = (n-1)/4$. Applying Theorem 2, we have that $\frac{n-1}{4} - \frac{R(n)}{2n} = \frac{a-1}{4} + \frac{1}{2}S$. We need $(a-1)/4 + S/2 = 0$ or $(a-1)/2 + S = 0$. As each of $(a-1)/2$, S is nonnegative, each must be zero. Hence $a = 1$, which means that n is squarefree. For the sum S to be zero, n must have no

divisors congruent to 3 modulo 4. This means that n must be a squarefree product of primes of the form $4k+1$.

Now suppose $n \equiv 3 \pmod 4$. Then $\lfloor n/4 \rfloor = (n-3)/4$, and $\frac{n-3}{2} - \frac{R(n)}{n} = \frac{a-3}{2} + S$, so we need $(a-3)/2 + S = 0$. As the sum S is nonnegative, we must have $(a-3)/2 \leq 0$, or $a \leq 3$. If $a = 3$ then $(a-3)/2 = 0$, so the sum S must be zero. But as 3 divides n, the sum S will be positive, so we cannot have $a = 3$. As n is odd, this leaves only the case $a = 1$, whence $(a-3)/2 = -1$, and $S = 1$. As $n \equiv 3 \pmod 4$, n is divisible by at least one prime p of the form $4k+3$. This prime cannot be 3, as then S would not be an integer. We claim that at most one prime divides n. Suppose to the contrary that two distinct primes, p and q, divide n, where p is of the form $4k+3$. If q is of the form $4k+1$, then terms of S include, at least, $e_p h(-p)$ and $e_{pq} h(-pq)$. Each of these terms is at least 1, so S is at least 2. Similarly, if q is of the form $4k+3$, then terms of S include, at least, $e_p h(-p)$ and $e_q h(-q)$, each of which is at least 1, so S is, again, at least 2. As a is 1, n is squarefree, and so n is a prime $p > 3$ of the form $4k+3$ for which $h(-p) = 1$. That is, n is one of 7, 11, 19, 43, 67, or 163, which is Shirali's empirical list.

While Shirali did not ask about even n, we can show that there are no even n with $\lfloor n/4 \rfloor = R(n)/(2n)$. If $n \equiv 0 \pmod 4$, then $\lfloor n/4 \rfloor = n/4$ so, by Theorem 2, $a/2 + S = 0$. As $a/2$ is positive, and the sum S is nonnegative, there can be no solutions. If $n \equiv 2 \pmod 4$, then $\lfloor n/4 \rfloor = (n-2)/4$ and $(a-2)/2 + S = 0$. If $a = 1$, then $(a-2)/2 = -1/2$, so $S = 1/2$. But this can only happen if 4 divides n, which does not happen in this case. If $a = 2$, then n is congruent to 0 modulo 4, not to 2. For any a larger than 2, $(a-2)/2$ is positive, so the sum $(a-2)/2 + S$ cannot be zero. So there are no solutions to $\lfloor n/4 \rfloor = R(n)/(2n)$ other than those found by Shirali.

Solutions to $(n-1)/4 - R(n)/2n = 1$

Shirali shows that $n = 25b$, where b is a squarefree product of primes of the form $4k+1$, is always a solution to $(n-1)/4 - R(n)/2n = 1$, and empirically he found solutions $n = pq$ where p and q are distinct, and each is taken from

the list 7, 11, 19, 43, 67, 163. We will show that these are, in fact, the only odd solutions, and we will find all of the even solutions.

By Theorem 2, if $(n-1)/4 - R(n)/2n = 1$, then $(a-1)/4 + S/2 = 1$, or $(a-1)/2 + S = 2$. As S is nonnegative, we must have $a \leq 5$. We will go through cases $a = 1$ to $a = 5$ in turn. First let $a = 1$, so $S = 2$. Then n is squarefree, and is either an odd number or twice an odd number. Now, 3 cannot divide n, or S would not be an integer. But there must be at least one prime p of the form $4k+3$ that divides n, otherwise S would be zero. We claim that there cannot be more than two odd primes that divide n. Assume, to the contrary, that p, q, r are distinct odd primes that divide n, where p is of the form $4k+3$. Then $e_p h(-p) \geq 1$. Also, either q or pq is congruent to 3 modulo 4, so one of $e_q h(-q)$ or $e_{pq} h(-pq)$ is in the sum S, and is at least 1. The same holds for r. Thus, if n is divisible by three or more odd primes, S is at least 3. So n is divisible by at most two odd primes.

If exactly one odd prime p divides n, then n is p or $2p$, where $p > 3$ is of the form $4k+3$. In either case, $S = e_p h(-p) = h(-p)$. As there are no primes p so that $h(-p) = 2$, as can be seen from the Appendix, there are no solutions for $a = 1$ with n divisible by exactly one odd prime. (In fact, for p a prime of the form $4k+3$, $h(-p)$ is always odd [8, Ch. XI, Theorem 6].)

Now suppose n is divisible by exactly two odd primes. Then $n = pq$ or $n = 2pq$ where p is of the form $4k+3$. If q is of the form $4k+1$, $S = e_p h(-p) + e_{pq} h(-pq) = h(-p) + h(-pq)$, while if q is of the form $4k+3$, then $S = e_p h(-p) + e_q h(-q) = h(-p) + h(-q)$. In the former case, we would have to have $h(-p) = h(-pq) = 1$, and there are no such pairs of primes p, q (see the Appendix). In the latter case, we need $h(-p) = h(-q) = 1$, and this occurs only when p and q are distinct primes from the list 7, 11, 19, 43, 67, 163, which are exactly the cases Shirali found empirically.

Now suppose $a = 2$. We have $(a-1)/2 = 1/2$, so $S = 3/2$, and $n = 4b$, where b is squarefree. Now b must be a prime, because if b is divisible by two distinct primes, say p and q, then 4, $4p$, $4q$, and $4pq$ all divide n and are congruent to 0 modulo 4, so S would be at least $7/2$. Also, b cannot be a

prime p of the form $4k+3$, because then 4, p, and $4p$ all divide n, and the sum is again too large. So b is either 2 or a prime of the form $4k+1$. When $b=2$, we get a solution, $n=8$. If b is a prime p of the form $4k+1$, then $S = e_4 h(-4) + e_{4p} h(-4p) = 1/2 + h(-4p)$. But there are no primes p of the form $4k+1$ so that $h(-4p)=1$. So the only new solution for $a=2$ is $n=8$.

Next consider $a=3$. Then 3 divides n, and S is not an integer. But $S=1$, so there are no solutions with $a=3$. If $a=4$, then $n=16b$, which is divisible by, at least, 4, 8, and 16. Thus S is at least $5/2$, and there can be no solutions.

Finally, consider $a=5$. Then $n=25b$, where b is squarefree. As $(a-1)/2=2$, we have $S=0$. Thus b must be a product of primes of the form $4k+1$, or 2 times such a product.

To recapitulate, this proves that all of the solutions to $(n-1)/4 - R(n)/2n = 1$ are $n=25b$ or $n=50b$, where b is a squarefree product of primes of the form $4k+1$; $n=pq$ or $2pq$, where p and q are distinct members of the list 7, 11, 19, 43, 67, 163; and $n=8$. In particular, Shirali found all of the odd solutions.

Solutions to $\lfloor n/4 \rfloor - R(n)/2n = 1$

Arguments similar to those above show that $\lfloor n/4 \rfloor - R(n)/2n = 1$ if and only if one of the following applies (here p and q are distinct primes congruent to 3 modulo 4 and at least 7, and s is a prime congruent to 1 modulo 4):

- $n=25b$ where b is a squarefree product of primes congruent to 1 modulo 4,
- $n=pq$ where $h(-p)=h(-q)=1$ (p, q = 7, 11, 19, 43, 67, 163 only)
- $n=p$ where $h(-p)=3$ (n = 23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907 only),
- $n=ps$ where $h(-p)=1$ and $h(-ps)=2$ (n = 35, 91, 187, 427 only).

In the first case there are infinitely many such n, while in each of the last three cases there are only finitely many solutions. To verify the above, the lists of discriminants with class numbers 1, 2, and 3 in the Appendix will be helpful.

Many similar equations can be readily solved using Schinzel's theorem.

On n so that $\sum_{i=1}^{\lfloor n/4 \rfloor} \left\lfloor \sqrt{in} \right\rfloor = \frac{n^2-1}{12}$

For $F(n) = \sum_{i=1}^{\lfloor n/4 \rfloor} \left\lfloor \sqrt{in} \right\rfloor$, Shirali gives a proof that $F(n) = \frac{n^2-1}{12}$ when n is a prime congruent to 1 modulo 4 [16, pp. 266–268]. For $n > 0$, let $n = a^2 b$ with b squarefree. Using Theorem 2 and arguments similar to those made by Shirali [16] it can be shown that:

$$\frac{n^2-1}{12} - F(n) = \begin{cases} \frac{S}{2} - \frac{n+2a}{8} & \text{for } n \equiv 0 \pmod 4, \\ \frac{S}{2} - \frac{a-1}{4} & \text{for } n \equiv 1 \pmod 4, \\ \frac{S}{2} + \frac{n-2a+2}{8} & \text{for } n \equiv 2 \pmod 4, \\ \frac{S}{2} + \frac{n-a}{4} & \text{for } n \equiv 3 \pmod 4. \end{cases} \tag{1}$$

Here, S is the sum defined following Theorem 2. Further below we prove the above formula for the case $n \equiv 3 \pmod 4$. The proofs of the other cases are similar.

From (1) we have that if n is a squarefree product of primes congruent to 1 modulo 4, and in particular if n is a prime of the form $4k+1$, then $F(n) = \frac{n^2-1}{12}$ (by the formula for the case $n \equiv 1 \pmod 4$, using $a = 1$ and $S = 0$). Thus, (1) includes Theorem 1 as a special case.

Consider now the question of whether there are any other n so that $F(n) = \frac{n^2-1}{12}$. From the above formulas, it is easy to see that if n is congruent to 0, 2, or 3 modulo 4, then $F(n) \neq \frac{n^2-1}{12}$. If $n \equiv 0 \pmod 4$, then to have $F(n) = (n^2-1)/12$, we would have to have $S/2 - (n+2a)/8 = 0$, or $S = (n+2a)/4$. But these cannot be equal because, for $n \equiv 0 \pmod 4$, S is not an integer, while $(n+2a)/4$ is an integer. The sum S is not an integer

because 4 divides n, so the term $e_4 h(-4) = 1/2$ is included in the sum S. The only other possible non-integral term in the sum S is $e_3 h(-3) = 1/3$, and whether or not this term is in the sum, S cannot be an integer. On the other hand, a is even because 4 divides n. So both n and $2a$ are divisible by 4, and $(n + 2a)/4$ is an integer.

For $n \equiv 2 \pmod 4$, $n - 2a + 2 \geq n - 2\sqrt{n} + 2 > 1$, while for $n \equiv 3 \pmod 4$, $n - a > 1$, so $F(n) \neq \frac{n^2-1}{12}$ in either of these cases.

When $n \equiv 1 \pmod 4$, the situation is more interesting. There are n that are congruent to 1 modulo 4 and are not squarefree products of primes of the form $4k + 1$, for which $F(n) = \frac{n^2-1}{12}$. A few examples are:

$245 = (5)(7^2)$, $605 = (5)(11^2)$,
$637 = (7^2)(13)$, $588245 = (5)(7^6)$,
$26420605 = (359^2)(5)(41)$, and $16526149049 = (2903^2)(37)(53)$.

This is not a complete list of solutions within the range covered by the examples. We just wanted to illustrate that not all examples are of the same "form."

It is not clear whether, overall, there is an easier way to characterize these values other than to note that these are the $n \equiv 1 \pmod 4$ for which $(a - 1)/2 = S$.

There is at least one pattern to the above solutions. That is that if T is a squarefree product of primes of the form $4k + 1$, and p is a prime of the form $4k + 3$, then $n = p^2 T$ is a solution if and only if $n = p^{2i} T$ is a solution for any integer $i \geq 0$. This can be proved by employing a classical formula given shortly below (Theorem 3) that relates class numbers of arbitrary discriminants to class numbers of *fundamental discriminants*. A *fundamental discriminant* D_0 is a nonsquare integer congruent to 0 or 1 modulo 4, where if $D_0 \equiv 1 \pmod 4$ then D_0 is squarefree, while if $D_0 \equiv 0 \pmod 4$ then $D_0 = 4d$ where d is squarefree and $d \equiv 2$ or $3 \pmod 4$. Any discriminant can be written uniquely as $D = f^2 D_0$ where D_0 is a fundamental discriminant. The following theorem relates class numbers of arbitrary discriminants to their associated fundamental discriminants [5, p. 228].

THEOREM 3. *For $D_0 < 0$ a fundamental discriminant, $f > 0$, and $D = f^2 D_0$ any discriminant*

$$\frac{h(D)}{\omega(D)} = \frac{h(D_0)}{\omega(D_0)} f \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \left(\frac{D_0}{p}\right)\frac{1}{p}\right).$$

where,

$\omega(x) = 2$ *for* $x \equiv 0$ *or* $1 \pmod 4$, *except* $\omega(-3) = 6$ *and* $\omega(-4) = 4$, *and*
$\left(\frac{D_0}{p}\right)$ *is the Kronecker symbol.*

For a prime p, the *Kronecker symbol* is

$$\left(\frac{D_0}{p}\right) = \begin{cases} 0 \text{ if } p \text{ divides } D_0, \\ 1 \text{ if } p \text{ is an odd prime and } D_0 \text{ is a quadratic residue of } p, \\ -1 \text{ if } p \text{ is an odd prime and } D_0 \text{ is not a quadratic residue of } p, \\ 1 \text{ if } p = 2 \text{ and } D_0 \equiv 1 \pmod 8, \\ -1 \text{ if } p = 2 \text{ and } D_0 \equiv 5 \pmod 8. \end{cases}$$

By (1), n is a solution to $F(n) = \frac{n^2-1}{12}$ for $n \equiv 1 \pmod 4$ exactly when $(a(n) - 1)/2 = S(n)$. To prove our assertion that $n = p^2T$ if and only if $n = p^{2i}T$ is a solution for any $i \geq 1$, we need to show that $\frac{a(p^2T)-1}{2} = S(p^2T)$ if and only if $\frac{a(p^{2i}T)-1}{2} = S(p^{2i}T)$. Now,

$$S(p^2T) = \sum_{j=1}^{s} e_{pt_j} h(-pt_j) = \sum_{j=1}^{s} h(-pt_j)$$

where the t_j, $1 \leq j \leq s$, are the positive divisors of T. Also,

$$S(p^{2i}T) = \sum_{k=0}^{i-1} \sum_{j=1}^{s} e_{p^{2k+1}t_j} h(-p^{2k+1}t_j) = \sum_{k=0}^{i-1} \sum_{j=1}^{s} h(-p^{2k+1}t_j)$$

Taking $D = -p^{2k+1}t_j$, $f = p^k$, and $D_0 = -pt_j$, Theorem 3 tells us that $h(-p^{2k+1}t_j) = p^k h(-pt_j)$. Then

$$S(p^{2i}T) = \sum_{k=0}^{i-1}\sum_{j=1}^{s} p^k h(-pt_i) = \left(\sum_{k=0}^{i-1} p^k\right)\left(\sum_{j=1}^{s} h(-pt_j)\right) \tag{2}$$

$$= \left(\sum_{k=0}^{i-1} p^k\right) S(p^2T).$$

Also $a(p^2T) = p$, and $a(p^{2i}T) = p^i$, so

$$\frac{a(p^{2i}T)-1}{2} = \frac{p^i-1}{2} = \left(\sum_{k=0}^{i-1} p^k\right)\frac{p-1}{2} = \left(\sum_{k=0}^{i-1} p^k\right)\frac{a(p^2T)-1}{2}. \tag{3}$$

From (2) and (3), and the fact that $\left(\sum_{k=0}^{i-1} p^k\right) \geq 1$, it follows that $\frac{a(p^2T)-1}{2} = S(p^2T)$ if and only if $\frac{a(p^{2i}T)-1}{2} = S(p^{2i}T)$.

We finish this section with a proof of (1) for the case $n \equiv 3 \pmod 4$. Now, if $k \leq \sqrt{in} < k+1$ then $\frac{k^2}{n} \leq i < \frac{(k+1)^2}{n}$, and if also $i \leq \frac{n-3}{4}$, then $k \leq \frac{n-3}{2}$ (for $n \equiv 3 \pmod 4$). For $1 \leq k \leq \frac{n-3}{2}$, $0 < \frac{(k+1)^2}{n} - \frac{k^2}{n} = \frac{2k+1}{n} \leq \frac{n-2}{n} < 1$, so $\left\lceil \frac{(k+1)^2}{n} \right\rceil - \left\lceil \frac{k^2}{n} \right\rceil$ is 1 or 0 depending on whether there is, or is not, an integer i satisfying $\frac{k^2}{n} \leq i < \frac{(k+1)^2}{n}$. As such, we can write

$$F(n) = \sum_{i=1}^{\lfloor n/4 \rfloor} \left\lfloor \sqrt{in} \right\rfloor = \sum_{i=1}^{\frac{n-3}{4}} \left\lfloor \sqrt{in} \right\rfloor = \sum_{k=1}^{\frac{n-3}{2}} k\left(\left\lceil \frac{(k+1)^2}{n} \right\rceil - \left\lceil \frac{k^2}{n} \right\rceil\right).$$

Expanding the rightmost sum, and collecting terms gives

$$F(n) = (-1)\sum_{k=1}^{\frac{n-3}{2}} \left\lceil \frac{k^2}{n} \right\rceil + \left(\frac{n-3}{2}\right)\left\lceil \frac{((n-1)/2)^2}{n} \right\rceil.$$

Now $\left\lceil \frac{x}{n} \right\rceil = \frac{x}{n} - \left\{\frac{x}{n}\right\} + 1$ if $n \not| x$ and $\left\lceil \frac{x}{n} \right\rceil = \frac{x}{n} = \frac{x}{n} - \left\{\frac{x}{n}\right\}$ if $n|x$. So

$$F(n) = (-1)\sum_{k=1}^{\frac{n-3}{2}} \frac{k^2}{n} + \sum_{k=1}^{\frac{n-3}{2}} \left\{\frac{k^2}{n}\right\} - \frac{n-3}{2} + \frac{a-1}{2} \tag{4}$$

$$+\left(\frac{n-3}{2}\right)\left\lceil\frac{((n-1)/2)^2}{n}\right\rceil.$$

The term $\frac{a-1}{2}$ is a "correction" to $\frac{n-3}{2}$ for the number of k, $1 \le k \le (n-3)/2$, so that $\frac{k^2}{n}$ is an integer. To see this, first observe that for $n = a^2b$, with b squarefree, $\frac{k^2}{n}$ is an integer if and only if ab divides k. The number of k so that $1 \le k \le (n-3)/2$ and ab divides k is $\left\lfloor\frac{(n-3)/2}{ab}\right\rfloor$. Now

$$\frac{(n-3)/2}{ab} = \frac{a^2b-3}{2ab} = \frac{a}{2} - \frac{3}{2ab} = \frac{a-1}{2} + \left(\frac{1}{2} - \frac{3}{2ab}\right),$$

so

$$\left\lfloor\frac{(n-3)/2}{ab}\right\rfloor = \frac{a-1}{2}.$$

Adding and subtracting a term $\left\{\frac{((n-1)/2)^2}{n}\right\}$ to (4) we obtain

$$F(n) = (-1)\sum_{k=1}^{\frac{n-3}{2}}\frac{k^2}{n} + \sum_{k=1}^{\frac{n-1}{2}}\left\{\frac{k^2}{n}\right\} - \left\{\frac{((n-1)/2)^2}{n}\right\} \tag{5}$$

$$-\frac{n-3}{2} + \frac{a-1}{2} + \left(\frac{n-3}{2}\right)\left\lceil\frac{((n-1)/2)^2}{n}\right\rceil.$$

It is easy to verify that

$$\frac{((n-1)/2)^2}{n} = \frac{n-3}{4} + \frac{n+1}{4n},$$

where, for $n \equiv 3 \pmod 4$, $n > 0$, $\frac{n-3}{4}$ is an integer and $0 < \frac{n+1}{4n} < 1$. So

$$\left\lceil\frac{((n-1)/2)^2}{n}\right\rceil = \frac{n-3}{4} + 1 = \frac{n+1}{4}, \text{ and } \left\{\frac{((n-1)/2)^2}{n}\right\} = \frac{n+1}{4n}.$$

Because $\sum_{j=1}^{m} j^2 = m(m+1)(2m+1)/6$, it follows that

$$\sum_{k=1}^{\frac{n-3}{2}} \frac{k^2}{n} = \frac{((n-3)/2)\,((n-1)/2)\,(n-2)}{6n}.$$

Also,

$$\sum_{k=1}^{\frac{n-1}{2}} \left\{ \frac{k^2}{n} \right\} = \frac{R(n)}{2n} = \frac{n-a}{4} - \frac{1}{2}S.$$

Substituting into (5) gives

$$F(n) = \frac{-\left((n-3)/2\right)\left((n-1)/2\right)(n-2)}{6n} + \frac{n-a}{4} - \frac{1}{2}S$$
$$-\frac{n+1}{4n} - \frac{n-3}{2} + \frac{a-1}{2} + \left(\frac{n-3}{2}\right)\left(\frac{n+1}{4}\right),$$

which simplifies to

$$F(n) = \frac{n^2-1}{12} - \left(\frac{n-a}{4}\right) - \frac{1}{2}S.$$

Acknowledgements

I thank Robin Chapman and Keith Matthews for contributions that made this article possible, and Andrzej Schinzel for communicating his theorem to me.

References

[1] Steven Arno, The imaginary quadratic fields of class number 4, *Acta Arith.* **60** (1992), 321–334.

[2] Steven Arno, M. L. Robinson, and Ferrell S. Wheeler, Imaginary quadratic fields with small odd class number, *Acta Arith.* **83** (1998), 295–330.

[3] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[4] Daniel Bump, *Automorphic Forms and Representations*, Cambridge University Press, Cambridge, UK, 1997.

[5] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer–Verlag, New York, 1992.

[6] Henri Cohen et al., PARI, freeware available at http://www.parigp-home.de/.

[7] Harvey Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer–Verlag, New York, 1978.

[8] Harvey Cohn, *Advanced Number Theory*, Dover, New York, 1980.

[9] David A. Cox, *Primes of the Form* $x^2 + ny^2$, John Wiley & Sons, New York, 1989.

[10] Dorian Goldfeld, Gauss' class number problems for imaginary quadratic fields, *Bull. Amer. Math. Soc.* **13** (1985), 23–37.

[11] Hugh L. Montgomery and Peter J. Weinberger, Notes on small class numbers, *Acta Arith.* **24** (1974), 529–542.

[12] Joseph Oesterlé, Nombres de classes des corps quadratiques imaginaries, *Séminaire Nicolas Bourbaki*, 1983–1984, Éxp. 631.

[13] George Pólya and Gábor Szegö, *Problems and Theorems in Analysis*, Volume 2, Fourth Edition, Springer–Verlag, New York, 1971.

[14] Paulo Ribenboim, *My Numbers, My Friends*, Springer–Verlag, New York, 2000.

[15] Andrzej Schinzel, An extension of some formulae of Lerch, *Acta Math. Inform. Univ. Ostraviensis* **10** (2002), 111–116.

[16] Shailesh A. Shirali, A Family Portrait of Primes – A Case Study in Discrimination, *Mathematics Magazine* **70** (1997), 263–272.

[17] Ian Stewart and David Tall, *Algebraic Number Theory*, Second Edition, Chapman & Hall, London, 1987.

[18] Christian Wagner, Class Number 5, 6, and 7, *Math. Comp.* **65**, No. 214 (April, 1996), 785–800.

Appendix A: Negative discriminants with class numbers 1, 2, 3, and factorizations

Class number 1 (All $D > 0$ for which $h(-D) = 1$):

3 (3),	4 (2^2),	7 (7),	8 (2^3),	11 (11),
12 (2^2)(3),	16 (2^4),	19 (19),	27 (3^3),	28 (2^2)(7),
43 (43),	67 (67),	163 (163).		

Class number 2 (All $D > 0$ for which $h(-D) = 2$):

15 (3)(5),	20 (2^2)(5),	24 (2^3)(3),	32 (2^5),	35 (5)(7),
36 (2^2)(3^2),	40 (2^3)(5),	48 (2^4)(3),	51 (3)(17),	52 (2^2)(13),
60 (2^2)(3)(5),	64 (2^6),	72 (2^3)(3^2),	75 (3)(5^2),	88 (2^3)(11),
91 (7)(13),	99 (3^2)(11),	100 (2^2)(5^2),	112 (2^4)(7),	115 (5)(23),
123 (3)(41),	147 (3)(7^2),	148 (2^2)(37),	187 (11)(17),	232 (2^3)(29),
235 (5)(47),	267 (3)(89),	403 (13)(31),	427 (7)(61).	

Class number 3 (All $D > 0$ for which $h(-D) = 3$):

23 (23),	31 (31),	44 (2^2)(11),	59 (59),	76 (2^2)(19),
83 (83),	92 (2^2)(23),	107 (107),	108 (2^2)(3^3),	124 (2^2)(31),
139 (139),	172 (2^2)(43),	211 (211),	243 (3^5),	268 (2^2)(67),

283 (283), 307 (307), 331 (331), 379 (379), 499 (499),
547 (547), 643 (643), 652 $(2^2)(163)$, 883 (883), 907 (907).

Appendix B: Schinzel's full theorem

In [15], Schinzel proves the theorem below. First we establish his notation.

$$E^*(x) = \begin{cases} x - \frac{1}{2} & \text{if } x \in \mathbb{Z}, \\ \lfloor x \rfloor & \text{otherwise.} \end{cases}$$

$$\phi(z,d) = \begin{cases} \sqrt{d} \sum_{\nu=1}^{\infty} \left(\frac{\nu}{d}\right) \frac{\cos 2\nu z\pi}{\nu\pi} & \text{if } d \equiv -1 \pmod 4, \\ \sqrt{d} \sum_{\nu=1}^{\infty} \left(\frac{\nu}{d}\right) \frac{\sin 2\nu z\pi}{\nu\pi} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

$$c_d = \begin{cases} 1/3 & \text{if } d = 3, \\ 1/2 & \text{if } d = 4, \\ 1 & \text{otherwise.} \end{cases}$$

$$\phi_1(z,d) = \begin{cases} \sqrt{d} \sum_{\nu=1}^{\infty} \left(\frac{d}{\nu}\right) \frac{\sin 2\nu z\pi}{\nu\pi} & \text{if } d \equiv 0,\ 1 \pmod 4, \\ 0, & \text{otherwise} \end{cases}$$

$$\phi_{-1}(z,d) = \begin{cases} \sqrt{d} \sum_{\nu=1}^{\infty} \left(\frac{-d}{\nu}\right) \frac{\cos 2\nu z\pi}{\nu\pi} & \text{if } d \equiv 0,\ -1 \pmod 4, \\ 0, & \text{otherwise.} \end{cases}$$

Then we have

THEOREM. *For m, n coprime positive integers and for all $x \in \mathbb{R}$*

$$\sum_{a=0}^{n-1} \left(E^* \left(x + \frac{a^2 m}{n} \right) - \left(x + \frac{a^2 m}{n} \right) \right)$$

$$= -\frac{n}{2} + \sum_{n=dd'} \left(\left(\frac{d}{m} \right) \phi_1 \left(d'x, d \right) + \left(\frac{-d}{m} \right) \phi_{-1} \left(d'x, d \right) \right).$$

COROLLARY 1. *For m, n coprime positive integers*

$$\sum_{a=0}^{n-1} \left\{ \frac{a^2 m}{n} \right\} = \frac{n-q}{2} - \sum_{\substack{d \mid n \\ d \equiv 0,\ 3 \pmod 4}} c_d \left(\frac{-d}{m} \right) h(-d)$$

where q^2 is the greatest square dividing n, $q > 0$.

In the main body of this article, we use Corollary 1 with $m = 1$.