A Counterexample for Germain

William C. Waterhouse

In 1804, Sophie Germain (1776–1831) began a correspondence with Carl Friedrich Gauss (1777–1855). She began by writing under a male pseudonym [**BD**, Chap. 3], discussing topics in the *Disquisitiones Arithmeticae* [**DA**] that he had published in 1801. When she disclosed her identity to him, in 1807, he wrote a response that is famous for its comments on the obstacles women face in learning mathematics. But less attention has been paid to the actual mathematical content of the letter, where (apart from giving a brief account of some of his current work) Gauss points out a mistake in one of the results Germain had sent him and gives a counterexample. In a recent little note on the topic [**MK**], MacKinnon has drawn attention to the large size of the number involved (13 digits), saying "When I saw it I was filled with wonder and suspicion. Is Gauss being less than honest with Germain about the frequency of counter-examples? Surely he could never have found such a monster as a lowest counter-example?" MacKinnon found one smaller example but correctly noted that it has a special nature that might have made it inappropriate, and he concludes that he cannot see how Gauss could have discovered the example he gave. The question was echoed by Wagon [**W**, 319].

What I have written here is a kind of detective story in which we try to discover what really happened. We do not have the original note by Germain, so we must first reconstruct the relevant part of it from what Gauss says. Then we can go on to figure out what reasoning would have led Gauss to a counterexample. There will be a fair amount of evidence for the validity of our reconstruction; in particular, his actual counterexample will be the first one that this method would produce. I shall summarize most of the mathematics needed, so I hope that readers can also use this paper as a sort of offbeat introduction to number theory.

1. THE COUNTEREXAMPLE AS GAUSS GAVE IT. Here is the relevant part of Gauss's letter, in my translation from the original French [**G**, 70–74].

> The taste for abstract science in general, and especially for the mysteries of numbers, is very rare; this is no surprise, as the enchanting charms of this lofty science only reveal themselves in their full beauty to those with the courage to go deeply into it. Women, by our customs and prejudices, must encounter infinitely more obstacles and difficulties than men do to acquaint themselves with these thorny investigations; and when a person of that sex is nonetheless able to break through these barriers and penetrate the most hidden secrets, she must undoubtedly have the most noble courage, quite extraordinary talent, and superior genius. Your favoring this science, which has added so much beauty and joy to my life, reflects honor upon it; nothing could give me a more flattering and unambiguous proof that its attractions are not chimerical.
>
> The learned notes with which your letters are so richly filled have given me countless pleasures. I have studied them with attention, and I am struck by the ease with which you have penetrated all branches of Arithmetic and perceived how to generalize and improve them. I beg you to take it as a proof of my attention if I dare to add a remark on one point in your last letter.

It seems to me that the converse proposition, that is, '*if the sum of the nth powers of two numbers is of the form hh + nff, the sum of the numbers themselves will be of that same form*,' is stated a bit too generally. Here is an example where this rule fails:

$$15^{11} + 8^{11} = 8\,649\,755\,859\,375 + 8\,589\,934\,592$$
$$= 8\,658\,345\,793\,967 = 1\,595\,826^2 + 11 \times 745\,391^2.$$

Yet $15 + 8 = 23$ cannot be reduced to the form $xx + 11yy$.

The same is true for the proposition: *if one of the factors of the formula yy + nzz (where n is a prime number) is of the form* $(1, 0, n)$, *the other necessarily belongs to the same form*. Your proof only shows that no other *indeterminate* form, besides those equivalent to $(1, 0, n)$, can give the product $(1, 0, n)$ when multiplied by the form $(1, 0, n)$; but this proof does not carry over to specific numbers. For determinant $-n$, let C be any class of forms that it is not equivalent to the principal class or to any *anceps* class; let D be the class resulting from duplication of C (which will be different from the principal class); and finally let D' be the class opposite to D. It follows that the composition $C + C + D'$ yields the principal class. Thus if the two numbers f, g can be represented by a form of the class C, and the number h can be represented by a form of the class D', the product $fg \times h$ can be reduced to $(1, 0, n)$; but it is easy to see that fg reduces not only to D or D' but also to $(1, 0, n)$. Thus here we have a case where one factor fg and the product $fg \times h$ are of the form $(1, 0, n)$ without the other factor having to be of that form. One can also see easily that the first factor must be composite; otherwise, the proposition would be true. In the example above, the factor $(15^{11} + 8^{11})/23$ contains the divisor 67.

2. RECONSTRUCTION OF THE ORIGINAL ASSERTIONS. There are some good clues in this letter that allow us to reconstruct the context of the original assertions. First, the end of the paragraph about forms refers back to the numerical example. Hence we can suppose that the mistake analyzed in that paragraph was in fact the fault in the argument for the earlier assertion. Furthermore, as Gauss explicitly cites the second result as assuming n prime, we can suppose that Germain also made that assumption in the first proposition. Indeed, as MacKinnon pointed out, there are many simple counterexamples otherwise.

The second clue is that Gauss describes the faulty result as a *converse* proposition. Thus presumably there was an earlier result stated the other way around; and since Gauss did not object to it, that result must be true. The hypotheses, therefore, must make the following statement true:

If $a + b = x^2 + ny^2$ for some x and y, then the same is true of $a^n + b^n$.

We already know we want n prime, and the values $a = 1, b = 2$ show that we want $n > 2$. It is (and was then) well known that the product of two numbers of the form $x^2 + ny^2$ is again of that form; explicitly,

$$(x^2 + ny^2)(x_1^2 + ny_1^2) = (xx_1 - nyy_1)^2 + n(xy_1 + yx_1)^2. \tag{1}$$

For odd n, we know that $a + b$ divides $a^n + b^n$ formally, and so we probably want to see when the quotient has the form $x^2 + ny^2$.

Now we can begin to get our bearings. Suppose n is an odd prime. In modern terms, Gauss had shown that the field generated over the rationals by the n-th roots of unity contains $\sqrt{\pm n}$; here we must take the plus sign when n is of the form $4k + 1$ and the minus sign when n is of the form $4k + 3$. One explicit consequence of this is in [**DA**, Article 357], where Gauss derives a decomposition

$$4 \cdot \frac{x^n - 1}{x - 1} = Y^2 \mp nZ^2. \tag{2}$$

These Y and Z are polynomials in x with integer coefficients, and they can be computed explicitly for any particular odd prime n. Formula (2) suggests that the direct theorem should assume that n is of the form $4k + 3$. Indeed, for (say)

$n = 5$, we can easily check that neither $3^5 + 2^5 = 275$ nor $2^5 + (-1)^5 = 31$ can be written as $Y^2 + 5Z^2$, though $3 + 2$ and $2 + (-1)$ can be. The direct theorem then must have been as follows.

Theorem A. *Let n be a prime of the form $4k + 3$. If $a + b = x^2 + ny^2$ for some x, y, then the same is true of $a^n + b^n$.*

The case $n = 3$ is special, because the quotient is already quadratic (see [**MK**]), so let us see how to prove this theorem for $n > 3$. The *Disquisitiones* notes that the highest term in Y is $2x^{(n-1)/2}$, and Z has no term that high. Setting $x = 0$, we have $4 = Y(0)^2 + nZ(0)^2$; hence the constant term in Y is ± 2 and the constant term in Z vanishes. Letting x approach 1, we get $4n = Y(1)^2 + nZ(1)^2$, so $Y(1) = 0$ and $Z(1) = \pm 2$. Hence an even number of terms with odd coefficients occur in each of Y and Z.

Now set $x = -a/b$; clearing denominators, we get a polynomial identity expressing $4(a^n + b^n)/(a + b)$ as a square plus n times a square. For $n = 11$, for instance, the formula in (2) is given explicitly in [**DA**], and it yields the identity

$$4 \cdot \frac{a^{11} + b^{11}}{a + b} = (-2a^5 + a^4b + 2a^3b^2 + 2a^2b^3 + ab^4 - 2b^5)^2 + 11(a^4b - ab^4)^2. \tag{3}$$

Our analysis of highest terms and constant terms shows in general that the terms in the squared quantities involving purely a or b are even, and there are an even number of others having odd coefficients. It follows that, whether a and b are even or odd, the two squares are even. Hence we can divide to get $(a^n + b^n)/(a + b)$ as a square plus n times a square. The theorem then follows from (1).

This proof was well within Germain's grasp. Her first letter to Gauss [**S**, 298–302; **BD**, 21] specifically singled out the decomposition of $(x^n - 1)/(x - 1)$ for praise, and at the end of her life she published a further note on that topic [**G**]. Thus we can be fairly sure that Theorem A was indeed her direct theorem. The converse theorem therefore must have read something like this:

(Supposed) Theorem B. *Let n be a prime of the form $4k + 3$. If $a^n + b^n$ is of the form $x^2 + ny^2$, the same is true of $a + b$.*

Germain may or may not have realized that even numbers pose a special problem. For $n = 7$, for instance, 2 is not of the form $x^2 + 7y^2$, and yet we have $2^7 + 0^7 = (4)^2 + 7(4)^2$. A related counterexample with $n = 7$ and a and b both positive was found by MacKinnon [**MK**, 350]. More generally, if n is of the form $7 + 16k$, we have $8(1 + 2k) = 1 + n$. We can then write

$$(2)^n + (4k)^n = 2^{n-3} \cdot 8(1 + 2k) \cdot \frac{1 + (2k)^n}{1 + 2k}.$$

By (1) and Theorem A, this quantity is of the form $x^2 + ny^2$; but $2 + 4k$ is not, as it is less than n and is not a square. This difficulty, however, turns out to be restricted to the prime 2. Indeed, as we shall see, Theorem B is true for $n = 7$ so long as $a + b$ is odd. To give the theorem the benefit of the doubt, we should therefore assume that $a + b$ is odd.

To simplify a bit more, we can note that factors equal to n are irrelevant. Indeed, as $n = (0)^2 + n(1)^2$, we know by (1) that a product nr is of the form

$x^2 + ny^2$ whenever r is of that form. Conversely, if $x^2 + ny^2 = nr$, then we see that n must divide x. Setting $z = x/n$, we get $r = y^2 + nz^2$. Hence we may as well assume that $a + b$ is not divisible by n. The same then will be true of $a^n + b^n$, as $a^n + b^n \equiv (a + b)^n \bmod n$. (That is, the difference of the sides is divisible by n.) Thus we may concentrate on the following version of the converse:

(Supposed) Theorem B′. *Let n be a prime of the form $4k + 3$, and suppose $a + b$ is not divisible by 2 or n. If $a^n + b^n$ is of the form $x^2 + ny^2$, the same is true of $a + b$.*

3. QUADRATIC FORMS AND THEIR COMPOSITION. To understand the discussion in Gauss's letter, we need to review a bit of his theory of quadratic forms. I shall use the notation common nowadays (see for instance **[D]**, **[B]**, **[BS]**, or **[C]**); it is slightly different from that of Gauss, but it does not introduce any serious conceptual differences.

The *forms* are polynomials $aX^2 + bXY + cY^2$ with a, b, c all integers. An integer t is *represented* by such a form if $t = ax^2 + bxy + cy^2$ for some integers x, y. Such a form is *equivalent* to the forms obtained as

$$a(pX + qY)^2 + b(pX + qY)(rX + sY) + c(rX + sY)^2$$

where p, q, r, s are integers and $ps - qr = \pm 1$ (the condition allowing us to reverse the integral change of variables). Those forms obtained by such a change of variables with $ps - qr = 1$ are called *properly* equivalent. Since the change of variables is invertible, a number represented by one form is also represented by all equivalent forms. The number $D = b^2 - 4ac$ is called the *discriminant* of the form; it is easy to compute that equivalent forms have the same discriminant. A form is called *primitive* if there is no nontrivial common divisor of its coefficients, and again this property is preserved under equivalence.

When the form is positive for all nonzero X and Y, like $X^2 + nY^2$, then D is negative. There is then a straightforward procedure (as efficient as the Euclidean algorithm) to reduce each form to a properly equivalent form satisfying the inequalities $-a \le b < a$ and $a \le c$, with $a \ne c$ when $b \ne 0$. Using this, you can easily see that there are only finitely many different proper equivalence classes with a given discriminant D. In fact, it is also true that no two of these "reduced" forms are properly equivalent, and so for any D we can routinely determine the different proper equivalence classes. For instance, if $D = -44$, there are four classes, corresponding to the reduced forms $X^2 + 11Y^2$, $3X^2 + 2XY + 4Y^2$, $3X^2 - 2XY + 4Y^2$, and $2X^2 - 2XY + 6Y^2$. The first three are primitive.

The simplest way to get a change of variables with $ps - qr = -1$ is to change the sign of one variable; this amounts to changing the sign of the central coefficient b, and the result is called the *opposite* form. If two forms are properly equivalent, so are their opposites, and thus we have an operation on classes. Forms in the class of the *principal* form $X^2 + nY^2$ (which is $(1, 0, n)$ in Gauss's notation) are properly equivalent to their opposites. If forms in another class have this property, the class is called *ambiguous*, or (in Gauss's Latin) *anceps*.

In the previous section, we wrote out a formal identity (1) giving the product of $(x^2 + ny^2)$ and $(x_1^2 + ny_1^2)$. For $D = -44$, here are two more identities:

$$(3x^2 + 2xy + 4y^2)(3x_1^2 + 2x_1y_1 + 4y_1^2) = 3r^2 - 2rs + 4s^2 \quad \text{with}$$

$$r = xx_1 + 2xy_1 + 2yx_1 \quad \text{and} \quad s = -xx_1 + xy_1 + yx_1 + 2yy_1, \tag{4}$$

and

$$(3x^2 + 2xy + 4y^2)(3x_1^2 - 2x_1y_1 + 4y_1^2) = u^2 + 11v^2 \quad \text{with}$$
$$u = 3xx_1 - xy_1 + yx_1 - 4yy_1 \quad \text{and} \quad v = xy_1 + yx_1. \tag{5}$$

We can think of these as ways of composing two forms with the same D to get another one. Such expressions exist in general, but there is a very subtle difficulty involved. Clearly, for instance, we could take (4) and change the sign of y_1, getting a valid identity with corresponding changes of signs in the expressions for r and s. Thus we would get expressions of the product in (5) by the two inequivalent forms $X^2 + 11Y^2$ and $3X^2 - 2XY + 4Y^2$. Gauss discovered that if we put suitable sign restrictions on the coefficients in the expressions of the new variables like r and s, then in fact the proper equivalence class of the form giving the product will depend only on the proper equivalence classes of the two factors. Thus we get a *composition* of proper equivalence classes. (Formulas (4) and (5) satisfy the restrictions.) A composite of primitive classes is primitive, and in modern terms the primitive proper equivalence classes form a commutative group under composition. The identity element is given by the principal class, and the opposite of a form is in the inverse class. Composing a form with itself is what Gauss called *duplication*. Formulas (4) and (5) show that the group for $D = -44$ is cyclic of order 3.

Finally, we need one fact about representations.

Lemma. *Let M be relatively prime to $4n$, and write $M = K^2M_0$ where M_0 has no repeated factors. Then M is represented by some form of discriminant $-4n$ if and only if there is some number r with $r^2 + n$ divisible by M_0.*

Proof: If such an r exists, then the form $M_0X^2 + 2rXY + ((r^2 + n)/M_0)Y^2$ has discriminant $-4n$ and represents M (with $Y = 0$). For the converse, say $M = ax^2 + bxy + cy^2$ with $b^2 - 4ac = -4n$. Clearly then b is even. Let d be the greatest common divisor of x and y, and find s and t with $sx + ty = d$. Direct computation using our expression for M shows that

$$M(as^2 - bst + ct^2) = (s(xb/2 + yc) - t(xa + yb/2))^2 + (ac - b^2/4)(sx + ty)^2.$$

Dividing by d^2 and observing that $ac - b^2/4 = n$, we see that n plus a square is divisible by M/d^2 and hence by M_0.

The converse part of this argument was given right at the start of Gauss's treatment of forms [**DA**, Art. 154]. Still earlier material [**DA**, Art. 105] shows that such an r exists if and only if, for every prime p_i dividing M_0, there is some r_i with $r_i^2 + n$ divisible by p_i. A simple count of powers now shows the following result:

Theorem C. *Let $M = BC$ be a number relatively prime to $4n$. If M and B are represented by forms of discriminant $-4n$, so is C.*

This may well have been in Germain's note. Observe that every number represented by a non-primitive form has a factor in common with the discriminant, and so only primitive forms will be candidates for representing M. If there is just one proper equivalence class of primitive forms (necessarily the principal class), then of course it follows that when M and B are of the form $x^2 + ny^2$, the same is true of the other factor C. This is true for $n = 3$ and for $n = 7$, and thus Germain's Theorem B′ is true when n is 3 or 7.

4. LOCATING THE ERROR. The lemma above shows that M_0 will be represented by a form of discriminant $-4n$ precisely when the primes in it are so represented. When a prime number (different from 2 and n) is represented by a form of discriminant $-4n$, it is represented by forms in a unique equivalence class [**DA**, Art. 168]; but that usually means forms in two (inverse) proper equivalence classes. Occasionally, of course, only one proper class occurs; this happens precisely when the class is (principal or) ambiguous. We can use the representations of the primes to build up a representation of a general M by compositions. Since we can choose either of the two classes (when they are distinct), we usually get several different classes of forms that represent the same number M. It is the distinction between equivalence and proper equivalence that makes this happen, and thus it is one of the more subtle parts of the theory. And it was here that Germain made her mistake. Gauss says explicitly that she tried to prove something like this:

(Supposed) Theorem D. *If $M = BC$ is prime to $4n$ and both M and B are represented by $X^2 + nY^2$, then so is C.*

As we saw, she could correctly have proved that C is represented by some primitive form of discriminant $-4n$. To derive Theorem D (and thus Theorem B′), she would then have to show that this form was in the principal class. It appears that she tried to do this using the group structure on the classes. As Gauss says, it is indeed true that there is no *formal composition* for any other form; that is, if we have an identity

$$f(x, y)(x_1^2 + ny_1^2) = u^2 + nv^2$$

with u and v bilinear combinations of x, y, x_1, y_1 as before, then $f(x, y)$ must be in the principal class [**DA**, Art. 249]. But because representations of the same number can be built up to come from different classes, the formal argument fails to establish a corresponding result for specific numbers.

Following Gauss's suggestion, we can easily find explicit counterexamples to Theorem D as soon as we find an n where not all the classes are ambiguous. The first such case is $n = 11$. Take, for instance, the first three primes represented by $3X^2 + 2XY + 4Y^2$ (and hence not by $X^2 + 11Y^2$); they are

$$\begin{aligned} 3 &= 3(1)^2 + 2(1)(0) + 4(0)^2 \\ 5 &= 3(1)^2 + 2(1)(-1) + 4(-1)^2 \\ 23 &= 3(1)^2 + 2(1)(2) + 4(2)^2. \end{aligned} \tag{6}$$

In Gauss's notation at the end of Section 1, these numbers will be f, g, and h. Direct composition of the first two, as in (4), gives us

$$15 = 3 \cdot 5 = 3(-1)^2 - 2(-1)(-2) + 4(-2)^2.$$

Composition of that result with the expression for 23, as in (5), gives us

$$3 \cdot 5 \cdot 23 = (13)^2 + 11(-4)^2.$$

But we can reverse a sign to get the other expression

$$5 = 3(1)^2 - 2(1)(1) + 4(1)^2;$$

and composing this with the expression for 3, as in (5), gives

$$15 = (2)^2 + 11(1)^2.$$

Thus both 15 and $15 \cdot 23$ are represented by $X^2 + 11Y^2$, but 23 is not.

This example also shows that, if we have primes represented by $3X^2 + 2XY + 4Y^2$, we can combine them either in pairs or in triples to get numbers represented by $X^2 + 11Y^2$. By (1), then, it is easy to see that we actually have the following result:

Theorem E. *Let M be a number that is not divisible by* 2 *or* 11. *Suppose $M = p_1 \cdot p_2 \cdots p_r$ is a product of primes each representable by a form of discriminant* -44. *Then M is represented by $X^2 + 11Y^2$ except when there is* exactly one *of the p_i not represented by $X^2 + 11Y^2$.*

5. LOCATING A COUNTEREXAMPLE. We have shown by example that the supposed Theorem D is false. It was used in the argument for Theorem B′, and thus that proof is invalid, but we do not yet know that Theorem B′ is false. How might Gauss have searched for a counterexample? It would be most natural to try following the same pattern; that is, we should try to take $a + b$ to be a prime represented by $3X^2 + 2XY + 4Y^2$. We know $(a^{11} + b^{11})/(a + b)$ is represented by $X^2 + 11Y^2$, and Theorem E shows that we just need to have it divisible by some other prime p that is represented by $3X^2 + 2XY + 4Y^2$. We can also recall Fermat's result (see [**WL**]) that such a p will have to be of the form $11k + 1$. (The point is that there is an $x \not\equiv 1$ with $ax \equiv -b \bmod p$; then if p divides $a^{11} + b^{11}$, we have $x^{11} \equiv 1 \bmod p$. But $x^{p-1} \equiv 1$ by Fermat's theorem, and so 11 divides $p - 1$.) Thus our previous work gives us the following way of searching for an example:

1) Take a prime represented by $3X^2 + 2XY + 4Y^2$, and write it in all ways as a sum $a + b$.
2) Take another prime p of the form $11k + 1$ represented by $3X^2 + 2XY + 4Y^2$.
3) Test whether a^{11} is congruent to $-b^{11}$ modulo p.

When the congruence holds, then both p and $a + b$ will divide $a^{11} + b^{11}$, and Theorem E will tell us that $a^{11} + b^{11}$ is represented by $X^2 + 11Y^2$.

The first primes represented by $3X^2 + 2XY + 4Y^2$ are 3, 5, and 23. The first ones also of the form $11k + 1$ are 23 and 67. Obviously $a + b = 3$ and $p = 23$ should be tried first. The only decomposition is $a = 2$, $b = 1$. It is easy to compute powers modulo a small number, and we find that $2^{11} \equiv 1 \bmod 23$. Thus there is no example there. Similarly, we see that $4^{11} \equiv 1 \equiv 1^{11} \bmod 23$ and $3^{11} \equiv 1 \equiv 2^{11} \bmod 23$, so we have no examples with $p = 23$ and $a + b = 5$. We next move to $p = 67$, trying first $a + b = 3$ and then $a + b = 5$. There are still no solutions. But we have a wider range of possibilities with $a + b = 23$; and if we start from $b = 1$ and work our way up, we do find an example, at $b = 8$, $a = 15$. I repeat that checking these facts requires only computations of powers modulo 67, which are quite easy. (They are trivial if you have once computed a "table of indices" modulo 67, as described in [**DA**, Art. 58] and given in [**DA**, Table 1].) Thus relatively simple computation has led us to the following result, which we have fully established:

Theorem F. *The number* $15^{11} + 8^{11}$ *is represented by* $X^2 + 11Y^2$, *but* $15 + 8 = 23$ *is not.*

To confirm that we have been on the right trail, we can now observe that the one thing Gauss mentioned about his counterexample was that $(15^{11} + 8^{11})/23$ is divisible by 67.

6. COMPUTING THE COUNTEREXAMPLE. Gauss could have stopped at this point in his work, but it is not surprising that he did not. He was always fond of computation, and the counterexample will clearly be more immediately convincing if it is displayed rather than deduced. Furthermore, he had available a quite simple method for finding the expression of $15^{11} + 8^{11}$ as a square plus 11 times a square; it merely applies suitable compositions to the formula that started the whole discussion.

Let us recall what we know. First, we have

$$15^{11} + 8^{11} = 23 \cdot 67 \cdot M$$

for some integer M. (You can compute that $M = 5\,618\,653\,987$.) If we can represent M as $3X^2 + 2XY + 4Y^2$, then we can compose that representation with representations of 23 and 67 to get $15^{11} + 8^{11}$ as $X^2 + 11Y^2$.

It is in fact possible to take the value of M and solve this representation question from scratch (see Section 7.2). But we can do much better here, because we already have an expression for $67M$. Indeed, setting $a = 15$ and $b = 8$ in formula (3) above, we get

$$67M = (15^{11} + 8^{11})/23 = (-227\,723)^2 + 11(171\,780)^2. \tag{7}$$

Now we can work backwards: if we have $M = 3x^2 + 2xy + 4y^2$, and $67 = 3(3)^2 - 2(3)(4) + 4(4)^2$, composition gives us the expression $67M = u^2 + 11v^2$ with $u = 5x - 13y$ and $v = 4x + 3y$. We can solve to get $x = (3u + 13v)/67$ and $y = (-4u + 5v)/67$. Having (7), we try $u = \pm 227\,723$ and $v = \pm 171\,780$ to find values making x and y integers. Taking both u and v positive, we get the solution

$$M = 3(43\,527)^2 + 2(43\,527)(-776) + 4(-776)^2. \tag{8}$$

All we need to do now is to compose the terms differently, first combining

$$23 = 3(1)^2 + 2(1)(2) + 4(2)^2 \quad \text{and}$$
$$67 = 3(3)^2 + 2(3)(-4) + 4(-4)^2$$

to get

$$23 \cdot 67 = 3(7)^2 - 2(7)(-17) + 4(-17)^2.$$

Composing this then with (8), we get

$$15^{11} + 8^{11} = 23 \cdot 67 \cdot M = X^2 + 11Y^2,$$

where

$$X = 3(43\,527)(7) - (43\,527)(-17) + (-776)(7) - 4(-776)(-17) = 1\,595\,826$$

and

$$Y = (43\,527)(-17) + (-776)(7) = -745\,391.$$

Thus we have recovered exactly the example Gauss gave, and we have done it by methods all drawn from **[DA]**.

7. SIDE ISSUES

7.1. We can find a substantially smaller example if we are willing to allow one of a and b to be negative (there is nothing gained by taking them both negative).

Indeed, if we resume the search in Section 5 with $p = 23$ and $a + b = 3$, we observe that $4^{11} \equiv 1 \bmod 23$. Then we deduce as before that $4^{11} + (-1)^{11}$ is represented by $X^2 + 11Y^2$, while of course 3 is not. Readers might enjoy using the method from Section 6 to find the explicit representation

$$4^{11} + (-1)^{11} = 3 \cdot 23 \cdot 60\,787 = 82^2 + 11(617)^2.$$

It is also possible to find another positive example by continuing the search in Section 5 with $a + b = 23$ and $p = 67$; one finds that $a = 13, b = 10$ also works, and we have

$$13^{11} + 10^{11} = 1\,892\,160\,394\,037.$$

This is a little smaller than our previous example, but still of the same order of magnitude. The procedure of Section 6 shows us that

$$\frac{13^{11} + 10^{11}}{23} = (125\,212)^2 + 11(77\,805)^2,$$

whence

$$\frac{13^{11} + 10^{11}}{23 \cdot 67} = 3(20\,703)^2 + 2(20\,703)(-1\,669) + 4(-1\,669)^2$$

and finally

$$13^{11} + 10^{11} = (661\,539)^2 + 11(363\,634)^2.$$

7.2. We can use the value $M = 5\,618\,653\,987$ from Section 6 to illustrate the method Gauss gives [**DA**, Art. 322] for finding representations by $3X^2 + 2XY + 4Y^2$ from scratch. The first step is rather like that in Section 6; we observe that such an expression will give us

$$3M = Z^2 + 11Y^2 \quad \text{with} \quad Z = 3X + Y.$$

Thus it will suffice to find such representations of $3M$. There is an obvious bound

$$|Y| \leq \sqrt{3M/11} < 39\,146,$$

and any particular Y can be checked to determine whether $3M - 11Y^2$ is a square, but there are too many cases to check by hand.

Gauss's method now is a sort of sieve which he called the use of "eliminating numbers" and which is now called Gaussian exclusion [**B**, p. 194]. We take various small moduli E and determine conditions on Y modulo E that follow from the fact that $3M - 11Y^2$ is congruent to a square modulo E. For instance, in our case, take $E = 8$. We have $Y^2 \equiv 0, 1, 4 \bmod 8$, while we have $3M \equiv 1 \bmod 8$ and $-11 \equiv 5 \bmod 8$. Thus $3M - 11Y^2 \equiv 1, 6, 5 \bmod 8$. As only 1 among these is a square modulo 8, we see that $Y^2 \equiv 0 \bmod 8$, which tells us that Y is divisible by 4. Similarly, if we take $E = 25$, we have $3M - 11Y^2 \equiv 6^2(1 - Y^2) \bmod 25$, so we want $1 - Y^2$ to be congruent to a square. The squares modulo 25 are $0, \pm 1, \pm 4, \pm 6, \pm 9, \pm 11$. The condition on $1 - Y^2$ forces $Y^2 \equiv 0, 1 \bmod 25$, so we see that either Y is divisible by 5 or $Y \equiv \pm 1 \bmod 25$. Combining this result with divisibility by 4, we see that Y must have one of the following three forms:

$$Y = 20W, \quad Y = 100W + 24, \quad \text{or} \quad Y = 100W + 76.$$

Clearly this analysis has reduced the number of values to be checked; in the last two cases, for instance, we have $W \leq 320$. We can continue exclusion with other moduli until we feel the number of values is reasonable for checking. Gauss indicates that he was comfortable using up to 9 or 10 moduli, and that number of

steps will suffice here. For $Y = 100W + 24$, for instance, we may use moduli 3, 7, 13, 17, 19, 23, and 29; that leaves 10 values of W. The test at modulus 31 eliminates all W except 222, 239, and 304. These can be checked individually, and it turns out that none of them work. Similarly, for $Y = 100W + 76$, the moduli 3, 7, 13, 17, 19, 23, and 29 leave 12 values of W, and the test at modulus 31 eliminates all W but 7, 33, 126, 239, and 315, which we can check. It turns out that $W = 7$ works; we get

$$3M = (\pm 129\,805)^2 + 11(\pm 776)^2,$$

whence

$$M = 3(43\,527)^2 + 2(43\,527)(-776) + 4(-776)^2.$$

That, of course, is the solution we found earlier. If we want all solutions, we can attack the other case. For $Y = 20W$, we have $W \leq 1859$, and testing with the primes through 31 still leaves 25 values. The test at 37 cuts this down to 12 values, and the one at 41 then restricts W to be 538, 943, 944, 1541, or 1553. Again we can check these, and it turns out that 1553 works; we get

$$3M = (\pm 79\,019)^2 + 11(\pm 31\,060)^2,$$

whence

$$M = 3(36\,693)^2 + 2(36\,693)(-31\,060) + 4(-31\,060)^2.$$

Thus in fact there is also another representation of M. If we run through the computations for it, we get another expression for our basic counterexample:

$$15^{11} + 8^{11} = (935\,166)^2 + 11(841\,201)^2.$$

7.3. The computations in 7.2 could be shortened (using composition of forms) if we knew a factorization of M. But, as Gauss pointed out [**DA**, Art. 333], we can actually reverse that procedure and use our two different representations by $3X^2 + 2XY + 4Y^2$ to find factors of M. The proof of the lemma before Theorem C shows that each such representation can be rewritten to give a number whose square is congruent to -11 modulo M; specifically, if $rX + sY = 1$, then

$$[r(X + 4Y) - s(3X + Y)]^2 \equiv -11 \bmod M.$$

For the solution $X = 43\,527$, $Y = -776$, the Euclidean algorithm gives $r = -153$, $s = -8\,582$, and we get the congruence

$$(1\,107\,801\,791)^2 \equiv -11 \bmod M.$$

The solution $X = 36\,693$, $Y = -31\,060$ similarly gives the congruence

$$(3\,256\,684\,733)^2 \equiv -11 \bmod M.$$

Now whenever $u^2 \equiv v^2 \bmod M$, each prime dividing M divides either $u + v$ or $u - v$; and so long as $u \not\equiv \pm v \bmod M$, neither of $u \pm v$ is divisible by M itself. Thus we can find nontrivial factors of M as the greatest common divisors of $u + v$, M and of $u - v$, M. In our case, the Euclidean algorithm shows that the greatest common divisor of $3\,256\,684\,733 - 1\,107\,801\,791$ and M is 235 159, while that of $3\,256\,684\,733 + 1\,107\,801\,791$ and M is 23 893. And indeed you can check that

$$M = 235\,159 \cdot 23\,893.$$

REFERENCES

[B] D. A. Buell, Binary Quadratic Forms: Classical Theory and Modern Computations. Springer, New York, 1989.

[BD] L. L. Bucciarelli and N. Dworsky, Sophie Germain: An Essay in the History of the Theory of Elasticity. Reidel, Boston, 1980.

[BS] Z. I. Borevich and I. R. Shafarevich, Number Theory. Academic Press, New York, 1966 (Pure and Applied Math., No. 20).

[C] D. A. Cox, Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. Wiley, New York, 1989.

[D] H. Davenport, The Higher Arithmetic. Dover, New York, 1983.

[DA] C. F. Gauss, Disquisitiones Arithmeticae. First edition, 1801. Standard Edition = Werke, vol. I. Königliche Gesellschaft der Wissenschaften, Göttingen, 1863. English Translation, Springer, New York, 1986.

[G] C. F. Gauss, Werke, vol X.1. Königliche Gesellschaft der Wissenschaften and Teubner, Göttingen/Leipzig, 1917.

[GE] S. Germain, Note de la manière dont se composent les valeurs de y et z dans l'équation $4(x^p - 1)/(x - 1) = y^2 \pm pz^2$, et celles de Y' et Z' dans l'équation $4(x^{p^2} - 1)/(x - 1) = (Y')^2 \pm p(Z')^2$. J. Reine angew. Math. 7 (1831), 201–204.

[MK] N. MacKinnon, Sophie Germain, or, was Gauss a feminist?, Math. Gazette 74 (1990), 346–351.

[S] H. Stupuy, Oeuvres Philosophiques de Sophie Germain, Suivies de Pensées et de Lettres Inédites. Paris, Paul Ritti, 1879.

[W] S. Wagon, *Mathematica* in Action. Freeman, New York, 1991.

[WL] A. Weil, Number Theory: An Approach through History. Birkhäuser, Boston, 1984.

Department of Mathematics
The Pennsylvania State University
University Park, PA 16802

Is Algebra Useful?

I would like to share with you (and if you deem useful with the AMM readership) some considerations that occurred to me upon reading an article in the latest AMM issue.

At the end of his interesting article "Two-Year Magazine Subscription Rates" (Vol 100, #1, January 1993), Underwood Dudley states that "... it is better to present mathematics to students as a glorious adventure for the mind... That it has uses is important, but incidental. Few students will use it, but all can see some of its glory."

My initial reaction to this was one of incredulity: hasn't the author noticed that the majority of people fail to identify the glory of mathematics and are in fact proud to profess a deep disdain for it? That most people tolerate the math requirements in school only because of educators' assurances that one day those mathematical skills will be useful? Expecting students to take mathematics course to appreciate the glory of the subject would not be much different from expecting us to take pottery courses to appreciate the glory of human manipulative creation. Some would enjoy it (including me) but most would object to the rationale for imposing such an experience.

My dismay, however, slowly turned to keen interest in what this statement really means: finally somebody is realizing, and admitting, that much of what we mathematicians have imposed on society as an essential part of knowledge can in fact be dispensed with; that people can live meaningful, productive and happy lives without using any mathematics beyond grade 3; that we should start thinking seriously about who needs what mathematical knowledge; and that we should start providing real rationales for each of the topics we want to have taught at any level.

Debates have raged recently between popular media and mathematicians about whether algebra is really useful. The arguments brought forward in defense of algebra were quite convincing to me, until I realized that I understood them because I am a mathematician, but they would not have convinced me if I weren't.

Hopefully some of us have initiated a move away from our ivory tower and towards the real world, where people use math, high power math, when needed, but do away with it whenever possible. Do you think that I am wrong? Then ask yourself when was the last time you used mildly advanced techniques for any purpose that had nothing to do with your job.

I thank you for your attention and I look forward to hearing from you.

Dr. Roberto Bencivenga
Learning Assistance Centre
Red Deer College
Box 5005
Red Deer, Alberta
Canada, T4N 5H5