SUMS OF FOUR SQUARES

Richard T. Bumby
Rutgers University

1. 0. Introduction.

The main results to be presented here deal with representations as a sum of four squares. However, it is useful for purposes of exposition to consider the corresponding theorems for sums of two squares. Since these results are so familiar, and part of elementary courses, it may seem that these propositions are belaboring the obvious. However, there is a slight difference in emphasis from the usual treatment that will be useful in describing the generalization. There are two types of questions to be considered: *algorithmic* — how can one compute representations of a number as a sum of two or four (or possibly some other number) of squares? — and *enumerative* — is there a structure on the set of representations that allows their number to be determined in an elementary manner?

The algorithmic question is treated to a certain extent in elementary texts. At this level, only the question of representing primes is considered and the question of the speed of the algorithm is generally ignored. Nonetheless, the usual algorithm for sums of two squares is polynomial-time relative to finding a square root of -1 modulo the number to be represented. For sums of four squares, the situation is a little different. Some books give algorithms which, while similar to that for sums of two squares, fail to be polynomial-time. Other books modify the algorithm so that it becomes polynomial-time if one has found an expression of -1 as a sum of two squares modulo the number to be represented. Strangely, no comment seems to be made on this distinction although the speed of algorithms is generally considered an important problem at the present time. Furthermore, the emphasis in textbooks is entirely on the representation of primes. This goes back to the early work on the subject. The formula for producing representations of products from representations of the factors appears to reduce the question to that of representing primes. However, questions of computational complexity make it clear that there may be some benefits in avoiding factorization.

The development to be described here suggests that the proper role of factorization in the question of representation as a sum of four squares occurs at the level of finding a representation of -1 as a sum of two squares modulo the number to be represented. Recently, I found an fast, sure and elementary procedure for fining such a representation modulo a prime (in many different ways). Thus, representing a number as a sum of four squares is no more difficult than factoring the number. It would be interesting to know its true complexity.

In some sense, the simpler problem of representations as a sum of two squares is more complicated. There are fast probabilistic algorithms for finding square roots modulo primes, which allows fast, but not sure, elementary computations of primes as a sum of two squares. In addition, the algorithm of Schoof [6] gives a deterministic polynomial time computation of a prime congruent to 1 mod 4 as a sum of two squares. This method is fast and sure, but I would not consider it to be elementary.

The enumerative question has been solved using modular forms. This allows exact formulas to be found for the number of representations of a number as a sum of 2, 4, 6 or 8 squares, and approximate formulas for representations as a sum of $2k$ squares for $k > 4$ (see [3]). Again, while these methods give good answers, they are far from elementary. In this article, I will show that the same method that answers the algorithmic question also provides an answer to the enumerative question. The new ingredient is a modification of the notion of "primitive representation". Actually, this is not new. The same method was studied by Aubry [1], but his work was so painfully elementary that it appears to have been ignored. It is cited in Dickson's *History*, so it was easy enough to discover that these results had appeared — after they had been rederived. Unfortunately, Aubry gives no references to the literature, and other references found through Dickson have not shed any light on developments leading to this approach.

Preliminary investigations suggest that these results can be extended to sums of 2^k squares, and possible to sums of any even number of squares. Although the construction of Pfister [4] works only for quadratic forms over fields, it appears possible to modify it to allow the algorithmic and enumerative questions to be studied for sums of squares over the integers. For the enumerative question, one expects that only results concerning the number of representations by genus of forms will be obtained.

One notational matter: congruence will be denoted by an ordinary *equal sign*. The modifying phrase "(mod n)" already serves to alert the reader that equality is being tested in a factor ring of the ring of integers.

2. 1. Sums of two squares.

Definition. *If* $\mathrm{GCD}(x, y) = 1$, *the solution of* $x^2 + y^2 = m$ *is said to be "primitive".*

Proposition 1.

$$2s_2(n) = \sum\{s_1(d)s_2^{(0)}(e) : de = n\} \tag{1}$$

where $s_k(m)$ *is the number of representations of* m *as a sum of* k *squares and* $s_k^{(0)}(m)$ *is the number of such representations that are primitive.*

Proof. The left side counts $\{(\epsilon, X, Y) : \epsilon = \pm 1, n = X^2 + Y^2\}$ and the terms on the right side counts $\{(u, x, y) : d = u^2, e = x^2 + y^2, \mathrm{GCD}(x, y) = 1\}$.

Given $d = u^2$, and $e = x^2 + y^2$, then $de = (ux)^2 + (uy)^2$. Since $n = de$, a map from union of the sets counted by the right side of equation (1) to the set counted by the left side can be given by $\epsilon = \operatorname{sgn} u$, $X = ux$, $Y = uy$. The inverse is given by setting $u = \epsilon\,\mathrm{GCD}(X, Y)$ and then setting $x = X/u$ and $y = Y/u$. The fact that these are inverses follows by standard elementary number theory.

Proposition 2. *The number of primitive representations of m as a sum of two squares is four times the number of solutions of the congruence $z^2 = -1 \bmod m$.*

Proof. Again the proof is "bijective" (except for the factor of 4). We show that one-fourth of the number of primitive representations and the number of solutions of the congruences are each equal to the number of ideals of norm m containing an element of the form $z - i$.

Suppose that $m = a^2 + b^2$, represent the ordered pair of integers (a, b) by the Gaussian integer $a + bi$, and consider the ideal I that it generates. When a and b are relatively prime, m is the smallest rational integer in I, and I contains an element of the form $z - i$. Note that z is uniquely determined modulo m by I. Each ideal is principal and has exactly four generators, obtained by multiplying any one by a unit of the Gaussian integers. Thus, each generator of an ideal I of norm m gives a representation of m as a sum of two squares. If this representation were not primitive, so that $\mathrm{GCD}(a, b) = d > 1$, then d would divide every element in I which rules out the possibility that an element of the form $z - i$ lies in I.

Since $a^2 + b^2 = 0 \bmod m$, the congruence requires that $z^2 + 1 = 0 \bmod m$. The ideal gives a solution of the congruence. On the other hand, given m and z, form the Z submodule of G generated by m and $z - i$. The congruence, $z^2 + 1 = 0 \bmod m$, implies that this Z module is also closed under multiplication by i, so it is an ideal in G.

It is also the case that arithmetic in G can be performed effectively. One way of doing this is through "lattice reduction". This calls for replacing the basis $m, z - i$ by an equivalent basis in which the first element has smaller norm. This is easily done, since z may be replaced by the *element of least absolute value* in its residue class mod m. The norm of the resulting quantity is at most $\frac{m^2}{4} + 1$ while the norm of m is m^2. If $m \geq 2$, the former is at most half of the latter. If the interchange of the order of the generators is accompanied by multiplying by $\frac{z+i}{m}$ and multiplying the second element by -1, the new basis $\{\frac{z^2+1}{m}, (-z) - i\}$ has the same form as the original basis. When a generator of the latter ideal is found, multiply by $z - i$ and divide by $\frac{z^2+1}{m}$ to get a generator of the original ideal. This gives a recursive algorithm for finding the generator which terminates in $O(\log m)$ of these steps.

Remark. Lattice reduction in the plane is related to continued fractions. Some of the classical algorithms for writing numbers as a sum of two squares use continued fractions. An efficient version of such an algorithm is given by Brillhart [2]. To establish the connection between these algorithms, start from n which is to be expressed as a sum of two squares and z with $n | z^2 + 1$. Suppose that z has been reduced modulo n so that $-n/2 \leq z \leq n/2$. Define n' by $z^2 + 1 = nn'$, and form the matrix $\begin{pmatrix} n & z \\ z & n' \end{pmatrix}$ which is seen to have determinant $+1$. The Euclidean algorithm, applied to the first column, writes this matrix as a product of matrices of the form $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$. The sequence of entries a are the partial quotients in the continued fraction expansion of n/z. Since the matrix is symmetric, the sequence of partial quotients will be *palindromic*. This gives an expression of the original matrix in the form $M^t M$, and the first column of M gives a pair of elements, the sum of whose squares is n. This, together with a recipe for stopping the Euclidean algorithm when this column has been found, is to be found in [2]. The "lattice reduction" method described above amounts to multiplying this matrix on left *and* right by matrices inverting the steps in the continued fraction.

The number of solutions of $z^2 = -1 \bmod m$ is a multiplicative function of m, easily determined when m is a prime power.

The two propositions of this section are well-known and are the ingredients of a combinatorial proof of a formula for the number of representations of a number as a sum of two squares. They are sketched here to provide a guide to a similar result for sums of four squares in the next section.

3. 2. Sums of four squares .

The classical treatment of this problem is less satisfactory than that of the representation as a sum of two squares. This is due to the need to introduce the arithmetic of quaternions in order to copy the proof of the previous section. The quaternions which are integer combinations of $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ (which we shall call 'integer quaternions" form a non-maximal order in the algebra of rational quaternions. A version of the construction below, using a maximal order, appears in the paper of Rabin and Shallit [5]. Use of the maximal order introduces some unnecessary difficulties because of the more complicated nature of the group of units. The more complicated structure of the ideals in the ring used here turns out to cause no trouble. Furthermore, the application to counting representations was not mentioned by Rabin and Shallit. The algorithm given here for writing m as a sum of four squares is fast, once one has a solution of $x^2 + y^2 = -1 \bmod m$. In particular, the algorithm will be shown to be fast for prime values of m in a later section. The whole story can now be told fairly briefly.

To begin with, write quaternions as $(a + bi) + (c + di)\mathbf{j}$, which may be abbreviated $\alpha + \beta\mathbf{j}$ where α and β are complex numbers (for integer quaternions these are Gaussian integers). Note that $\beta\mathbf{j} = \mathbf{j}\overline{\beta}$. This plays an important role in computing with quaternions, For example: the conjugate of $\alpha + \beta\mathbf{j}$ is

$$\overline{\alpha + \beta\mathbf{j}} = \overline{\alpha} - \mathbf{j}\overline{\beta} = \overline{\alpha} - \beta\mathbf{j}$$

and the norm is

$$\mathrm{Norm}(\alpha + \beta\mathbf{j}) = (\alpha + \beta\mathbf{j})(\overline{\alpha + \beta\mathbf{j}}) = \alpha\overline{\alpha} + \beta\overline{\beta}.$$

Since each of $\alpha\overline{\alpha}$ and $\beta\overline{\beta}$ is a sum of two rational squares, norms of quaternions are sums of four rational squares.

Definition. If the Gaussian integer $\mathrm{GCD}(\alpha, \beta) = 1$, this representation will be called "j-primitive".

Proposition 3.

$$4s_4(n) = \sum\{s_2(d)s_4^0(e) : de = n\} \tag{2}$$

with notation as in the preceding section except that $s_4^{(0)}(e)$ is the number of j-primitive representations of e.

Proof. If $\gamma \in G$ has norm d and $\alpha + \beta\mathbf{j}$, with $\mathrm{GCD}(\alpha, \beta) = 1$ in G, has norm e, then $\gamma\alpha + \gamma\beta\mathbf{j}$ has norm de. This latter expression is unchanged if α and β are multiplied by a unit, ϵ of G and γ is divided by ϵ. The factor of 4 in the formula arises from the 4 choices for ϵ.

The inverse map is given by extracting a factor equal to a greatest common divisor of α and β in G for a given expression $\alpha + \beta\mathbf{j}$. This quantity must be a generator of the ideal spanned by α and β, so is uniquely determined up to multiplication by a unit of G. The construction can be made to look more like the corresponding result for sums of two squares if a canonical choice among the four generators of an ideal in G is made.

Remark. Note that $\frac{s_2(n)}{4}$ is a multiplicative function of n. It will be shown that $\frac{s_4^{(0)}(n)}{8}$ is also multiplicative, so that their convolution $\frac{s_4(n)}{8}$ will then be multiplicative.

In order to count the number of j-primitive representations of m, it will be necessary to compute with (right) ideals in the ring of integral quaternions. Ideals will turn out to either be principal or to be multiples of $(1 - \mathbf{i}, 1 - \mathbf{j})$. The latter type can be characterized as being ideals for a larger order. This means that the arithmetic of the ring of integral quaternions will behave as if all ideals were principal. Furthermore, this is effective. A lattice reduction argument can again be used to find a generator for any ideal.

Proposition 4. *The number of j-primitive representations of m as a sum of four squares is eight times the number of solutions of the congruence $x^2 + y^2 = -1 \bmod m$.*

Proof. Given a j-primitive expression $\alpha + \beta\mathbf{j}$ of norm m, look at the right ideal that it generates. As a module relative to the induced right action of G, it is generated by $\alpha + \beta\mathbf{j}$ and $-\beta + \alpha\mathbf{j}$. Since $\mathrm{GCD}(\alpha, \beta) = 1$ in G, it follows that the intersection of the module with $G = G\mathbf{1}$ is generated by $m = \alpha\overline{\alpha} + \beta\overline{\beta}$, and that the whole module is generated by m and an element of the form $\eta - \mathbf{j}$.

Conversely, any ideal containing $\eta - \mathbf{j}$ must contain $\eta\overline{\eta} + 1$, so that the intersection with G is generated by an element γ with $\mathrm{GCD}(\gamma, \eta) = 1$. The ideal also contains $(\eta - \mathbf{j})\overline{\gamma} = \eta\overline{\gamma} - \gamma\mathbf{j}$ and $\gamma\mathbf{j}$, so it contains $\eta\overline{\gamma}$. Since $\mathrm{GCD}(\eta, \gamma) = 1$, this means that $\gamma | \overline{\gamma}$. Thus the ideal generated by γ is ambiguous, so it is generated either by a rational integer or by a rational multiple of $1 + i$. In the latter case, the product of the ideal with $1 + \mathbf{j}$ is a multiple of $1 + i$, so that the ideal belongs to a larger order.

It remains to show that a G-module generated by a rational integer m and an element $\eta - \mathbf{j}$ with $m | \eta\overline{\eta} + 1$ is closed under right multiplication by $\mathbf{j}$. However,

$$(\eta - \mathbf{j})\mathbf{j} = 1 + \eta\mathbf{j} = (1 + \eta\overline{\eta}) - (\eta - \mathbf{j})\overline{\eta}.$$

Thus the values of η mod m with $\eta\overline{\eta} + 1 = 0$ mod m give the ideals whose intersection with G is generated by m. One should note that, while the right action of quaternions is used, the notion of primitivity is based on a left action of G which is different from the G-module structure obtained by restricting the right action.

This procedure gives what could be considered to be an elementary proof of a formula for the number of representations of m as a sum of four squares. In Proposition 4, it has been shown that this number is 8 times a multiplicative function of m. (The number of solutions of a congruence is multiplicative by the Chinese Remainder Theorem, and the multiplicativity of convolutions of multiplicative functions is a familiar exercise in elementary number theory.) A formula will follow from

Proposition 5. *The number of solutions of the congruence* $x^2 + y^2 + 1 = 0 \bmod p^k$ *is*

$$\begin{array}{rl} 1 & (\text{all } p, k = 0) \\ 2 & (p = 2, k = 1) \\ 0 & (p = 2, k > 1) \\ (p-1)p^{k-1} & (p = 1 \bmod 4, k > 0) \\ (p+1)p^{k-1} & (p = 3 \bmod 4, k > 0) \end{array}$$

Proof. The result for $m = 1, 2,$ or 4 can be obtained by inspection. Since there are no solutions when $m = 4$, there can be no solutions for any multiple of 4. For odd primes p, the number of solutions of $\text{Norm}(\alpha) = a$ mod p for any integer a is equal to the number of elements in $\left(\frac{\mathbf{F}_p[x]}{(x^2+1)}\right)^*$ divided by the number of elements in $\mathbf{F}_p^*$, since the norm map is an epimorphism. This gives the stated result when $k = 1$. Hensel's lemma completes the proof.

Since the functions $\frac{1}{2}s_1()$, $\frac{1}{4}s_2^{(0)}()$, $\frac{1}{4}s_2()$, $\frac{1}{8}s_4^{(0)}()$ and $\frac{1}{8}s_4()$ are all multiplicative, the generating function of the form $\sum\{f(n)n^{-s} : n \geq 1\}$ will have an Euler product decomposition, allowing an expression in terms of the Riemann zeta function and Dirichlet L-functions. The theorems expressing some of these functions as convolutions of other functions give the generating functions as products of the corresponding generating functions. The results are summarized below. In the table, $\chi(p)$ is the character which is ± 1 with $p = \chi(p) \pmod 4$ for odd p and 0 for $p = 2$.

f	$\sum f(p^k)p^{-ks}$	
$\frac{1}{2}s_1$	$(1-p^{-2s})^{-1}$	
$\frac{1}{4}s_2^{(0)}$	$(1+p^{-s})(1-\chi(p)p^{-s})^{-1}$	
$\frac{1}{4}s_2$	$(1-p^{-s})^{-1}(1-\chi(p)p^{-s})^{-1}$	
$\frac{1}{8}s_4^{(0)}$	$(1+2^{1-s})$	$(p = 2)$
	$(1-\chi(p)p^{-s})(1-p^{1-s})^{-1}$	$(p \neq 2)$
$\frac{1}{8}s_4$	$(1-2^{-s})^{-1}(1+2^{1-s})$	$(p = 2)$
	$(1-p^{-s})^{-1}(1-p^{1-s})^{-1}$	$(p \neq 2)$

This agrees with the classical result that $\frac{1}{8}s_4(n)$ is the sum of the divisor of n that are not divisible by 4.

4. 3. Sums of two squares modulo primes. .

It remains to give an algorithm for solving $x^2 + y^2 = -1 \bmod p$. The motivation comes from an approach to finding square roots modulo p.

Notation: Let $p - 1 = 2^g \cdot h$ with h odd. For $a \bmod p$, let $\mathrm{Lev}(a) = \mathrm{LEAST}\{k : a^{2^k h} = 1\}$. Thus the elements for which $a^h = 1$ have $\mathrm{Lev}(a) = 0$ and, is c is a quadratic non-residue, then $\mathrm{Lev}(c) = g$.

In [7], Shanks describes an algorithm (which turned out to be older than its author) for solving $x^2 = a \bmod p$ whenever an element c is known with $\mathrm{Lev}(c) > \mathrm{Lev}(a)$. The algorithm is easily seen to be *fast*, and it is *sure* if an appropriate value of c is available. I would also consider it to be *elementary*. The discovery of a quadratic non-residue is fast in practice, but no *sure* way of finding one quickly is known without the assumption of appropriate Riemann hypotheses.

One implementation of the algorithm is based on maintaining an equation of the form $ax = y^2 \bmod p$ starting from $x = a^h$ and $y = a^{\frac{h+1}{2}}$. In particular, the order of x modulo p is a power of 2. The given element c is used to find an element u whose order modulo p is exactly $2^{1+\mathrm{Lev}(x)}$. Replacing y by yu and x by xu^2 preserves the conditions on x and y and lowers the value of $\mathrm{Lev}(x)$. When $\mathrm{Lev}(x) = 0$, the only possibility is $x = 1 \bmod p$, so that $a = y^2 \bmod p$.

If a quantity , c is known with $\mathrm{Lev}(c) > 1$, then $x^2 = -1 \bmod p$ can be solved. This x, with $y = 0$ gives a solution of $x^2 + y^2 = -1 \bmod p$. This means that we may confine attention to the case in which every number obtained in the following algorithm is at level 0 or 1. Such numbers can be written as $\pm u^2$ by an effective computation. It is convenient to write the equation we are trying to solve in the homogeneous form $x^2 + y^2 = -z^2$. We construct a finite sequence of numbers c_j — of length at most $C \log p$ — stopping when we get an element which is not at level 1. The numbers themselves are constructed, but, since they will all be at level 1, we may think of them as being of the form $-z^2 \bmod p$ for some z which can be computed. The bound on the number of elements in the sequence depends on the fact that one is constructing actual integers whose (archimedean) size is decreasing. This brings a little bit of *global* arithmetic (about as complicated as $1 + 1 = 2$) into the process.

The first number will be $c_0 = p - 1$. This is at level 1. Now,

$$c_{j+1} = \begin{cases} c_j/2 & \text{if } 2|c_j \\ c_j - 1 & \text{otherwise} \end{cases}$$

This process would set some $c_j = 1$ if it did not stop earlier, but $\mathrm{Lev}(1) = 0$, so the process can not only produce numbers at level 1. If it first produces an element at level 0, the equation $c_j = 1 + c_{j+1}$ or $c_j = c_{j+1} + c_{j+1}$ gives the element c_j at level 1 as a sum of two elements taken from $\{1, c_{j+1}\}$ at level 0. This solves the required congruence. We have also seen how to solve the congruence if an element of level greater than 1 is produced.

Remark. It should be noted that all algorithms described here have been tested for all values of $p < 2^{16}$. The original motivation involved testing various methods for discovering solutions of $x^2 = a \bmod p$. That analysis led to a different algorithm for discovering a solution of $x^2 + y^2 = -1 \bmod p$ which used only computations modulo p, but was more complicated in other ways than the present proof.

5. 4. References..

1. L. Aubry, Solution complète en entiers de $N = a^2 + b^2 + c^2 + d^2$; nombre des solutions avec a, b, c, d sans facteur commun, et nombre total des solutions, *Sphinx–Œdipe* 9, Numéro Spécial (March 1914), 1–14.
2. J. Brillhart, Note on representing a prime as a sum of two squares, *Math. Comp.* 26 (1972), 1011–1013.
3. E. Grosswald, *Representation of Integers as Sums of Squares*, Springer, 1985.
4. A. Pfister, Multiplikative quadratische Formen, *Arch. Math.* 16 (1965), 363–370.
5. M. O. Rabin and J. O. Shallit, Randomized algorithms in number theory, *Comm. Pure Appl. Math.* 39 (1986), 239–256.
6. R. J. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* 44 (1985), 483–494.
7. D. Shanks, Five number-theoretic algorithms, Proceedings of the second Manitoba conference on numerical mathematics, *Congr. Numer.* 7 (1973), 51–70.