C. Project Description
Forms in Many Variables over Local Fields

1. Introduction

A fundamental question in both number theory and mathematics as a whole is to determine whether an equation $f(x_1, \ldots, x_s) = 0$ with integral coefficients, or a system of such equations, has a solution in which all of the variables are integers. Unfortunately, it is known that there does not exist any algorithm which will determine whether an arbitrary system has such solutions. However, something can often be said for particular types of equations.

An important consideration when trying to determine whether a system has an integral solution is whether the equation has a solution in p-adic integers for each prime p. If no p-adic integral solution exists for some prime, then it is easy to show that there is no solution of the system in rational integers. One can therefore consider the existence of local solutions as giving "evidence" that a solution in rational integers might exist. In fact, in some situations a Hasse principle has been proven, showing that if p-adic solutions exist for all primes p, then solutions in rational integers do exist, or sometimes the p-adic solutions may be required to satisfy some property such as nonsingularity. Understanding the nature of p-adic solutions of equations is also a necessary prerequisite for applying the Hardy-Littlewood (circle) method for showing the existence of rational integral solutions of equations. When applying the circle method, one typically obtains a term, the *singular series*, which is related to the solutions of the equations modulo each positive integer. One usually needs to know that the singular series is bounded away from zero, and often one way to establish this involves either assuming or proving the existence of (a density of) p-adic solutions for each p.

One situation in which much can be said about the existence of p-adic solutions is when one seeks a zero of a form (homogeneous polynomial) or a simultaneous zero of a system of forms. A solution of such a system is said to be nontrivial if at least one of the variables is nonzero. A conjecture attributed to Artin stated that any system of R forms of degrees $k_1, \ldots, k_R$ whose coefficients are rational integers has a nontrivial p-adic solution for each p provided only that the number s of variables is at least $k_1^2 + \cdots + k_R^2 + 1$. Although results of Terjanian [33,34] show that this conjecture is not true even in the case of one form, there are two senses in which Artin was correct. First, a result of Brauer [6] shows that there does exist some function $g(k_1, \ldots, k_R)$ of the degrees such that a nontrivial p-adic solution exists for each p provided only that $s \geq g(k_1, \ldots, k_R)$. Also, work of Ax & Kochen [3] has shown that there is an integer $p(R; k_1, \ldots, k_R)$ such that if $p > p(R; k_1, \ldots, k_R)$ then Artin's conjectured bound does suffice to guarantee nontrivial integral solubility over $\mathbb{Q}_p$.

The proposed research explores problems related to Artin's conjecture. The main facet of the research is to study problems about systems of additive forms (i.e. those with no cross terms). The proposer plans to study both the number of variables required to guarantee solubility and also how large p needs to be to allow "nice" bounds to hold. Also, we intend to a lesser extent to study general forms, again both attempting to bound the number of variables needed to ensure solubility over $\mathbb{Q}_p$ and also searching for reasonable bounds for the function $p(R; k_1, \ldots, k_R)$ above, particularly in the case where $R = 1$.

In order to more fully describe the proposed research, a small amount of notation is necessary. Let $\mathbb{K}$ be a field. Given a system of additive forms of degrees $k_1, \ldots, k_R$ with rational integer coefficients, we will always assume that we have $k_1 \geq k_2 \geq \cdots \geq k_R$. We then define $\Gamma(R; k_1, \ldots, k_R; \mathbb{K})$ to be the least integer such that the system always has a nontrivial $\mathbb{K}$-integral solution whenever there are at least $\Gamma(R; k_1, \ldots, k_R; \mathbb{K})$ variables present. If $\mathbb{K} = \mathbb{Q}_p$, then we abbreviate this as $\Gamma_p(R; k_1, \ldots, k_R)$. We also define $\Gamma(R; k_1, \ldots, k_R)$ to be the maximum value of $\Gamma_p(R; k_1, \ldots, k_R)$ for all primes p, and note that the theorem of Brauer mentioned earlier guarantees that $\Gamma(R; k_1, \ldots, k_R)$ exists. When all of the degrees are equal, we further abbreviate our notation to $\Gamma_p(R; k)$ and $\Gamma(R; k)$.

2. Bounds on the Number of Variables

The proposer intends to continue his research into the number of variables necessary to ensure that a system of additive equations of equal degrees

$$\begin{array}{rcl} a_{11}x_1^k + \cdots + a_{1s}x_s^k & = & 0 \\ \vdots \qquad\qquad \vdots & & \vdots \\ a_{R1}x_1^k + \cdots + a_{Rs}x_s^k & = & 0, \end{array} \tag{1}$$

where the a_{ij} may be any rational integers, has a solution in p-adic integers for each prime p. This will involve refining and extending the methods of Davenport & Lewis [12,13,14], Low, Pitman & Wolff [26], Brüdern & Godinho [9,10], and possibly also those of Schmidt [29,30,31]. Let us discuss what has been done in the past on this problem, and indicate where we hope to either make improvements or add new results.

The earliest result on this problem was obtained by Davenport & Lewis [12], who showed that if there is only one form of degree k, then $k^2 + 1$ variables suffice to guarantee that the system has a nontrivial p-adic solution for each prime p. In other words, they showed that $\Gamma(1; k) \leq k^2 + 1$. Furthermore, they showed that this bound is sharp in the sense that if $k = p - 1$ for some prime p, then the equation

$$(x_1^k + \cdots + x_k^k) + p(x_{k+1}^k + \cdots + x_{2k}^k) + \ldots \\ + p^{k-1}(x_{(k-1)k+1}^k + \cdots + x_{k^2}^k) = 0$$

in k^2 variables has no nontrivial $\mathbb{Q}_p$-integral solutions.

The method used by Davenport & Lewis to bound $\Gamma(1;k)$ may be viewed as a three-step process. Since the majority of results in this field have been proven through a procedure similar to this one, we describe it here. We obtain the result by fixing a prime p and showing that $\Gamma_p(1;k) \leq k^2+1$. First, a normalization process is applied to the system which allows one to assume that each nontrivial integral zero of the system is nonsingular, and also to assume that certain numbers of variables are explicit when the form is viewed modulo powers of p. One can do this because the property of having singular zeros forces a particular polynomial in the coefficients of the system to become zero. If a result bounding $\Gamma(R;k)$ can be proven when this polynomial is nonzero, then the compactness of $\mathbb{Q}_p$ can be used to show that the result is still true when the function is equal to zero. Then by examining how the value of this function is affected by applying a nonsingular linear change of variables to the system, one can show that the assumptions about the equation modulo powers of p may be made. Next, one uses the information obtained by the normalization process to show that the equation has a nonsingular solution modulo a suitably high power of p. This step may require some ingenuity, and is where innovations leading to smaller bounds on $\Gamma(R;k)$ have typically been made. Finally, Hensel's lemma is used to lift the solution of congruences to a solution of (1) over $\mathbb{Q}_p$.

As we just mentioned, it is in the second part of this scheme where improvements have usually been made. Davenport & Lewis proved their result for $\Gamma(1;k)$ through their method of contractions – first finding a solution which is nonsingular modulo p, and then successively finding solutions nonsingular modulo powers of p until they reach a power high enough to employ a version of Hensel's lemma. Shortly thereafter, Davenport & Lewis [13] were able to use their methods to obtain the bounds

$$\Gamma(R;k) \leq [9R^2k\log(3Rk)]$$

for all odd k, and the bound

$$\Gamma(R;k) \leq [48R^2k^3 \log(3Rk^2)]$$

for all even k larger than 2. In their proof, they find their nonsingular solution essentially by assuming that the matrix of coefficients of (1) has many disjoint submatrices which are nonsingular modulo p, and obtain their final bound by calculating the number of variables in (1) necessary to ensure that these submatrices exist. Later, Low, Pitman & Wolff [26] improved on this bound, eliminating a factor of R. Recently, Brüdern & Godinho [9] have shown that

$$\Gamma(R;k) \leq R^3k^2$$

except when $R = 3$ and k is a power of 2, in which case they obtain $\Gamma(R;k) \leq 36k^2$. Note that this bound shows that it is possible to achieve the conjectured dependence on k for all exponents. The proposer [16] used a theorem due to Schanuel [27] about congruences modulo prime powers to improve the argument of Brüdern & Godinho, obtaining the bound

$$\Gamma(R;k) \leq 4R^2k^2$$

for all values of R and k. This bound is better than those of Low, Pitman & Wolff and Davenport & Lewis when k is even and suitably large in terms of R. The proposer intends to attempt to improve this bound, possibly by integrating the method of contractions used by Davenport & Lewis with the use of Schanuel's theorem.

While proving the result $\Gamma(R;k) \leq 4R^2k^2$, the proposer was also able to modify Schanuel's theorem to apply to finite extensions $\mathbb{K}$ of $\mathbb{Q}_p$. Inserting this modification into the proof yields the bound

$$\Gamma(R;k;\mathbb{K}) \leq R^2k^{2+2n(\log k)/(\log 2)},$$

where n is the degree of the extension. While the dependence on k is much larger than could be desired, this does show for the first time that one has $\Gamma(R;k;\mathbb{K}) \ll_{k,\mathbb{K}} R^2$. The previous best such bound was developed by Leep & Schmidt [22], who showed that $\Gamma(R;k;\mathbb{K}) \ll_{k,\mathbb{K}} R^{2^{k-1}}$. Unfortunately, the proposer's bound is weak in terms of k, especially in that the bound depends on the degree of the field extension. Bounds which do not depend on this degree are desirable since they immediately yield bounds in the case where $\mathbb{K}$ is an extension of $\mathbb{Q}_p$ of infinite degree. Birch [5] has recorded such a bound for $\Gamma(1;k;\mathbb{K})$, which is unfortunately also extremely large. While it is somewhat complicated to state, Birch's formula always gives a bound at least as large as $3^k k^{k-1}$. When $\mathbb{K}$ is an unramified extension of $\mathbb{Q}_p$, Dodson [15] has given the bound $\Gamma(1,k,\mathbb{K}) \leq 36k^2(\log k)^2$. Unfortunately, Dodson notes that his method cannot be directly extended to obtain a uniform bound when there is ramification. Skinner [32] has developed a bound which, while not depending on ramification, does depend on the shape of the degree of the form. In particular, he shows that if $\mathbb{K}$ is a finite extension of $\mathbb{Q}_p$ and $k = p^\tau$ for some integer τ, then

$$\Gamma(1;k;\mathbb{K}) \leq k((k+1)^{2\tau+1} - 1) + 1.$$

The proposer [18] has shown that Skinner's method extends directly to systems of equations, leading to the bound

$$\Gamma(R;k;\mathbb{K}) \leq Rk(Rk+1)^{2\tau+1}$$

when k and $\mathbb{K}$ are restricted as above. The proposer intends to attempt to obtain bounds for $\Gamma(R;k;\mathbb{K})$ which do not depend on the degree of $\mathbb{K}$ over $\mathbb{Q}_p$ and which are more reasonable than those of Birch. This will involve developing better methods to deal with the situation in which the prime p ramifies in $\mathbb{K}$.

The proposer also wishes to study the true manner in which $\Gamma(R;k)$ and $\Gamma(R;k;\mathbb{K})$ depend upon R. While there does not appear to be any good reason why one should not have $\Gamma(R;k) \ll_k R$, the best known bounds are of the form $\Gamma(R;k) \ll_k R\log R$. The proposer intends to attempt to obtain bounds on $\Gamma(R;k)$ which depend only linearly on the number of equations. Once this is accomplished, he will attempt to generalize these bounds to bounds on $\Gamma(R; k; \mathbb{K})$.

The proposer will also study the more general problem of bounding the quantity $\Gamma(R; k_1, \ldots, k_R)$ when the degrees are no longer required to all be equal. Wooley [36] has shown that $\Gamma(2; 3, 2) = 11$. For a system of R equations, Schmidt [31] has proven the bound

$$\Gamma(R; k_1, \ldots, k_R) \leq cR^2 4^{k_1} k_1^{22} \log k_1,$$

where c is an effectively computable constant and we recall that k_1 is the largest of the degrees. One also has the result

$$\Gamma(R; k_1, \ldots, k_R) \leq (k_1^2 + 1) \cdots (k_R^2 + 1)$$

due to Leep & Schmidt [22]. However, not much other work has been done specifically on this problem. Although theorems about the number of variables needed to guarantee nontrivial zeros of systems of general forms certainly apply to systems of diagonal forms, one feels that systems of diagonal forms should require fewer variables due to their special shape. On the other hand, Arkhipov & Karatsuba [2], Brownawell [8] and Lewis & Montgomery [25] have independently constructed systems of additive forms in exponentially many variables which have no nontrivial p-adic solutions for a given prime p. This sharpened earlier work of Arkhipov & Karatsuba [1].

The proposer [19] has contributed to this field by showing that if $k_1 > k_2$, then one has

$$\Gamma(2; k_1, k_2) \leq 128(k_1 + k_2)^2(k_1 - k_2)^2 - 2(k_1 + k_2).$$

Further, he has shown by different methods that if at least one of k_1 and k_2 is odd, then

$$\Gamma(2; k_1, k_2) \leq 2k_1^2 + k_2^2 + 1.$$

While the constant in the first bound is admittedly rather large, one can see that this bound is better than those of Schmidt and Leep & Schmidt when the degrees are large and close together.

The proposer intends to study several problems related to the situation in which the forms have different degrees. First, he would like to settle Artin's conjecture for two forms in the case in which at least one degree is odd. If both degrees are odd, then it should be possible to modify the proposer's previous work to obtain a bound smaller than $k_1^2 + k_2^2 + 1$, at least when k_1 and k_2 are large. It should be noted that work of Wooley [35] shows that the problem hinges on the values of $\Gamma_p(2; k_1, k_2)$ for "small" primes p. Hence for specific values of k_1 and k_2 it may be possible to obtain interesting results by focusing on these small primes. Also, the proposer would like to improve if possible the aforementioned bound on $\Gamma(2; k_1, k_2)$. If $k_1 = k_2 = k$, then work of Brüdern & Godinho [10] has come close to proving Artin's conjecture, showing that it is true except possibly for two families of degrees, and that one has $\Gamma(2; k) \leq 8k^2$ even in these cases. Since the conjecture is so close to being proven when $k_1 = k_2$, it seems plausible that the conjecture might hold if $k_1 \neq k_2$. However, knowing that exponential growth is required for general values of R makes the opposite conclusion seem plausible as well. It would be very interesting to determine the true state of affairs in this situation.

The proposer will also investigate what happens to $\Gamma(R; k_1, \ldots, k_R)$ when we remove the restriction that $R = 2$. While the proposer's work in the case of two forms does extend to the general case, preliminary investigations indicate that directly extending the method leads to bounds larger than those of Leep & Schmidt. Hence the proposer intends to either improve these methods or develop new methods to deal with this problem.

Additionally, the proposer intends to investigate the problem of bounding $\Gamma(R; k_1, \ldots, k_R)$ in the case in which $k_1, \ldots, k_R$ are all odd. While this can be thought of as a special case of the problem discussed in the previous paragraph, it is interesting enough to merit being mentioned on its own. This is because the examples showing that $\Gamma(R; k_1, \ldots, k_R)$ has exponential growth all require forms of even degree. In particular, the examples showing that exponential growth is required for additive forms over $\mathbb{Q}_p$ require many forms whose degrees are divisible by $p-1$. The proposer wishes to discover the extent to which exponential growth is required when none of the forms have even degrees, or even whether exponential growth is required at all in this situation.

Finally, the proposer would like to explore the number of variables required to guarantee p-adic solubility when the forms are not required to be diagonal. This would center, at least at first, on systems of forms of specific small degrees, such as two forms of degrees 2 and 3, or two forms each of degree 3. In the first situation, work of Leep & Schmidt [22] implies almost immediately that 23 variables suffice, although Artin's conjecture states that only 15 should be needed. In the second problem, the situation is much worse, as Wooley [37] has shown that 308 variables are enough, while Artin's conjecture says that 19 should suffice. It would be very interesting to know the true state of affairs in these situations, although it may be extremely difficult to make progress on these problems. It is also hoped that investigating these questions will lead to methods which will apply to general systems of forms, improving some of the bounds in this area.

3. Large Values of the Prime p

In an early attempt to prove Artin's conjecture, Birch & Lewis [4] were able to show that the conjecture is true for a single (not necessarily diagonal) form of degree 5 over $\mathbb{Q}_p$ provided that p is large enough. Shortly thereafter, Laxton & Lewis [21] proved a similar result for a form of degree either 7 or 11. Around the same time, Ax & Kochen [3] employed methods of mathematical logic to show that such a statement holds for systems of forms of any degrees. Later, Cohen [11] gave another proof of this result. However, none of these results give bounds on how large the prime p must be.

The first such bounds were found by Brown [7], who quantified the method of Cohen, showing that k^2+1 variables is sufficient for a single form of degree k over $\mathbb{Q}_p$ provided that

$$p > 2^{2^{2^{2^{2^{11^{k^{4k}}}}}}}.$$

One hopes that the true bounds on the function $p(R;k)$ are much smaller, and in fact Leep & Yeomans [24] showed a few years ago that $p(1;5) \leq 43$. More recently, the proposer [17] has quantified the work of Laxton & Lewis, showing that

$$p(1;7) \leq 2^7 5^{10} 7^5 17^3 \approx 1.03 \times 10^{17}$$

and

$$p(1;11) \leq 2^7 5^4 11^5 23^3 61^3 \approx 3.56 \times 10^{19}.$$

The key to the proposer's work is the use of a theorem due to Schmidt [28] giving a lower bound on the number of solutions of equations over a finite field.

The proposer intends to attempt to improve these bounds as far as possible. One way to accomplish this might be to develop a more convenient form of Schmidt's theorem. When Schmidt derives his lower bound, he obtains a rather small error term at the cost of increasing the number of elements in the finite field necessary to apply the theorem. By allowing the error term to be larger, one might be able to reduce the required size of the field, which is the limiting factor in the proposer's work. Another possibility is to extend the results of Leep & Yeomans [23] on quintic forms over finite fields to forms of higher degree. If this can be done successfully, there is a good chance that it will lead to better bounds than modifying Schmidt's theorem will.

The proposer also intends to attempt to develop methods to bound $p(1;k)$ for values of k larger than 11. The methods of Laxton & Lewis unfortunately depend on a certain combinatorial property of small numbers, and do not directly extend to forms of larger degree. It is conceivable that one can work around this problem through a modification of their normalization process. If this turns out to be impossible, then new methods will need to be developed to work on this problem.

It would also be interesting to attempt to prove results of this type for systems of forms. As was mentioned earlier, good candidates for study would be a system of two forms of degrees 2 and 3, or a system of two cubic forms. Unless Artin's conjecture is proven to be true in these situations, it would be very worthwhile to have some bound on the primes p for which there may be counterexamples.

One can also ask this type of question about systems of additive forms. Wooley [35] has shown that if $k_1 \geq k_2 \geq 1$ and p is a rational prime with $p > k_1^4 k_2^2$, then

$$\Gamma_p(2; k_1, k_2) \leq \begin{cases} 2(k_1 + k_2) + 1, & k_1 \geq k_2 > 1 \\ 2k_1 + 2, & k_1 > k_2 = 1 \\ 3, & k_1 = k_2 = 1. \end{cases}$$

This shows in particular that if both degrees are larger than 1 and p is large enough, then $2(k_1 + k_2) + 1$ variables suffice. Wooley then conjectures for systems of R additive forms that if all the degrees are at least 2 and k_1 is again the largest degree, then for all rational primes p satisfying

$$p > k_1^4 k_2^2 \cdots k_R^2,$$

one has

$$\Gamma_p(R; k_1, \ldots, k_R) \leq 2(k_1 + \cdots + k_R) + 1.$$

The proposer intends to attempt to prove this conjecture.

A consequence of Wooley's conjecture would be that for sufficiently large primes p, the quantity $\Gamma_p(R; k_1, \ldots, k_R)$ exhibits only polynomial growth rather than exponential growth. The proposer [20] has recently established this fact in the case where all of the degrees are different, proving that if $k_1 > k_2 > \cdots > k_R$ and $p \geq k_1 - k_R + 1$, then one has

$$\Gamma_p(R; k_1, \ldots, k_R) \leq \frac{3}{2}(k_1 + \cdots + k_R)^2$$

and that if $p \geq \max\{(k_1 - k_R)/2 + 1, k_2 - k_R + 1\}$, then one has

$$\Gamma_p(R; k_1, \ldots, k_R) \leq 2R(k_1 + \cdots + k_R)^2(k_1 - k_R)^2.$$

The proposer intends to extend this research in several different directions. First, it would be very desirable to extend these results to the situation where some of the forms may have the same degrees. The proposer's methods in their current form unfortunately break down in this situation. It may be possible to obtain results in this direction by using the normalization procedure used by Wooley in [36], although this would drive up the bound on $\Gamma_p(R; k_1, \ldots, k_R)$. Second, it would also be very desirable to decrease further the primes p for which we can still obtain a bound on $\Gamma_p(R; k_1, \ldots, k_R)$ which exhibits only polynomial growth, even if it were to be a polynomial of very high degree. Finally, the proposer wishes to study how large p needs to be to ensure that

$$\Gamma_p(R; k_1, \ldots, k_R) \leq k_1^2 + \cdots + k_R^2 + 1,$$

in other words, how large p needs to be so that Artin's conjecture is true for a system of additive forms.