HENSEL'S LEMMA AND THE SOLVABILITY OF DIOPHANTINE EQUATIONS

An Internal Assessment

For International Baccalaureate Mathematics Higher Level

Submission Date: March 18, 2019

Exam Session: May 2019

Contents

1. Definitions and Notation

We begin by defining key terms to be found in this report.

- "Solving the polynomial f" means finding points where $f = 0$.
- An expression "vanishes" when it equals 0.
- $a \mid b \implies a$ divides b; $a \nmid b \implies a$ does not divide b.
- $a \equiv b \pmod{m}$ is known as a "congruence," and implies that $m \mid a - b$. Also, the relation $a \not\equiv b \pmod{m} \implies m \nmid a - b$.
- $\mathbb{Z}/n\mathbb{Z}$ is the set of possible remainders when dividing integers by n (i.e., $\{0, 1, ..., n\}$).
- For an element a of $\mathbb{Z}/n\mathbb{Z}$, a^{-1} is the element such that $aa^{-1} \equiv 1 \pmod{n}$.
- $\mathbb{Z}^+$ denotes the positive integers.
- $\mathbb{Q}^\times$ denotes the non-zero elements of $\mathbb{Q}$.
- A field satisfies the properties listed in [4].

Date: July 2018.

- The characteristic of a field F is defined as the number of times the multiplicative identity must be added to itself to get the additive identity.
- $s \in S \implies s$ is an element of the set S.
- An element $x \in S$ is a square in $S \iff x = y^2$ has a solution $y \in S$.
- $A \setminus B$ is the set of all elements in A not in B.
- p is a positive prime in $\mathbb{Z}$.
- $\text{val}_p(n)$ is equal to the highest power of p dividing n.
- $\mathbb{Z}_p^\times$ is the set of all elements x in $\mathbb{Z}_p$ such that $\text{val}_p(x) = 1$.
- $F[X_1, X_2, ..., X_n]$ is the set of all polynomials in $X_1, X_2, ..., X_n$ with coefficients in F, where F is a field.
- A quadratic form is a polynomial $f \in \mathbb{Q}[X_1, X_2, \cdots, X_n]$ such that each term $c_i X_1^{a_{1i}} X_2^{a_{2i}} \cdots X_n^{a_{ni}}$ (for a constant c_i) satisfies

$$\sum_{i=0}^{n} a_{ji} \leq 2.$$

  for any fixed j. Further, there exists some $i = k$ such that equality holds.
- $f(X_1, X_2, ..., X_n)$ is a polynomial in variables $X_1, X_2, ..., X_n$.
- $f(X_1, X_2, ..., X_n)$ has a solution in $S \iff$ there exists an n-tuple $(X_1, X_2, ..., X_n)$ that solves f such that each $X_i \in S$.

2. Introduction

The study of rational solutions to a polynomial $f \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$ is a long standing branch of number theory that closely intermingles with concepts from algebraic geometry. Over the past few centuries, various methods have been developed to answer different questions that can arise in this study. In the 1900s, Hensel introduced a power expansion of rational numbers using primes as the base of each power, and ultimately a new number system, to help answer such questions. The usefulness of this number system wil come to light in §6.

Using this new number system, Hasse and Minkowski were able to develop one of the most elegant theorems that partially answers the existence of a rational solution to a rational polynomial. The aim of this report is to discuss the theory leading up to Hasse. This report also aims to make the notions Hensel introduced in the 20th century more natural. Thus, our ultimate goal is to uncover how the primes can be used in determining non-trivial rational solutions of polynomials.

My rationale in choosing this area of study in mathematics is because of its rich history and depth dating back . Furthermore, I am personally invested in self-studying pure mathematics, and such concepts are not accessible in a typical high school setting. The generalizations that are proved in this higher-level study are quite powerful and require focused self-study. I find that arguments made in this area of study are among the most elegant in all of mathematics.

3. The Congruence $x_k^2 - 2 \equiv 0 \pmod{7^{k+1}}$

We begin our study by analyzing a simple case: where f is a quadratic in one variable. We do not analyze the simpler cases where f is linear or constant in one variable, as these are trivial:

- $f(x) = ax + b$, $a \neq 0$ has solution $x = -\frac{b}{a}$.
- $f(x) = c$ has solutions at all values of x if $c = 0$ and has 0 solutions otherwise.

To develop the theory of prime numbers in finding rational solutions of f we analyze the function $f(x) = x^2 - 2$ and solve the modular congruence $x^2 \equiv 2 \pmod{7^k}$, where $k \in \mathbb{Z}^+$.

Proposition 3.1. *For any positive integer k, the congruence $x_k^2 - 2 \equiv 0 \pmod{7^{k+1}}$ has a solution $x_k \in \mathbb{Z}/7^{k+1}\mathbb{Z}$.*

Proof. Letting $k = 0$, the congruence $x_0^2 - 2 \equiv 0 \pmod{7}$ has solution $x_0 \equiv \pm 3 \pmod{7}$. We now proceed by induction to prove that this congruence is solvable for all positive integers k Assume that for $k = m$, $x_{m-1}^2 - 2 \equiv 0 \pmod{7^m}$ has a solution. We now show it has a solution for $k = m + 1$. I claim that $x_m \equiv x_{m-1} - \frac{f(x_{m-1})}{f'(x_{m-1})} \pmod{7^{m+1}}$. The division in this

modulus is allowed since $f'(x_{m-1}) \not\equiv 0 \pmod 7$. Substituting this value into $x_m^2 - 2$ we have:

$$\begin{aligned} x_m^2 - 2 &\equiv (x_{m-1} - \frac{f(x_{m-1})}{f'(x_{m-1})})^2 - 2 \pmod{7^{m+1}} \\ &\equiv (x_{m-1}^2 - 2) - 2x_{m-1}\frac{f(x_{m-1})}{f'(x_{m-1})} + (\frac{f(x_{m-1})}{f'(x_{m-1})})^2 \pmod{7^{m+1}} \\ &\equiv f(x_{m-1})[1 - \frac{2x_{m-1}}{f'(x_{m-1})}] + (\frac{f(x_{m-1})}{f'(x_{m-1})})^2 \pmod{7^{m+1}} \end{aligned}$$

Note that since $f'(x_{m-1}) = 2x_{m-1}$, the term in the brackets vanishes, and so we have $x_m^2 - 2 \equiv (\frac{f(x_{m-1})}{f'(x_{m-1})})^2 \pmod{7^{m+1}}$. Since $f(x_{m-1}) \equiv 0 \pmod{7^m}, (\frac{f(x_{m-1})}{f'(x_{m-1})})^2 \equiv 0 \pmod{7^{2m}}$ Since $m > 1$, we have that $(\frac{f(x_{m-1})}{f'(x_{m-1})})^2 \equiv 0 \pmod{7^{m+1}}$, so $x_m^2 - 2 \equiv 0 \pmod{7^{m+1}}$. Hence, for any positive integer k, the congruence $x_k^2 - 2 \equiv 0 \pmod{7^{k+1}}$ has a solution. □

4. Hensel's Lemma

The claim used in the proof of Proposition 3.1 seems unmotivated at first glance. Where would we come up with the idea to make such a substitution on x_m, and moreover, why should it even work? It turns out the claim uses Newton's Method, which is a way to approximate roots of polynomials. In fact, in the case of lifting solutions to higher powers of p, this approximation, along with certain assumptions, gives us exact roots of a polynomial modulo higher powers of p! To see this, we must first prove Taylor's Theorem:

Theorem 4.1. *(Taylor) Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree d. Then, for any $a \in F$, we have the polynomial identity*

$$f(x) = \sum_{k=0}^{d} \frac{f^{(k)}(a)}{k!}(x-a)^k,$$

where $f^{(k)}(a)$ denotes the kth derivative of f evaluated at $x = a$.

Proof. We begin with a lemma:

Lemma 4.2. *There exists constants $c_k \in F$ such that*

$$f(x) = \sum_{k=0}^{d} c_k(x-a)^k,$$

for any element $a \in F$.

Proof. Consider the system of equations set up by equating the coefficients of each power of x. That is, let $f(x) = \sum_{k=0}^{d} d_i x^i$. Let $e = d + 1$. We then have the following augmented matrix (with column i denoting the coefficients of c_{i-1} in the linear system):

$$\left[\begin{array}{ccccc|c} a_{11} & a_{12} & a_{13} & \dots & a_{1e} & d_0 \\ & a_{22} & a_{23} & \dots & a_{2e} & d_1 \\ & & \ddots & & \vdots & \vdots \\ & & & \ddots & \vdots & \\ 0 & & & & a_{ee} & d_e \end{array}\right]$$

where each $a_{ij}, d_k \in F$ and the a_i's are polynomial expressions in $c_0, c_1, \cdots c_d$. Because we are working over a field, we may solve for a_{ee} and back substitute up the matrix. From the bottom most row we may deduce the value of c_d. Moving one row up and substituting this value for c_d, we find the value of c_{d-1}. We continue upwards until we reach the value for c_0. Note that this process may require multiplication by an inverse as not all non-zero entries of the matrix may equal 1. Since we are working over a field, this process is allowed. Hence Lemma 4.2 is proven. □

We may now prove Theorem 4.1. Consider the expansion of f as in Lemma 4.2. Notice $f^{(k)}(a)$ gives us the coefficient of the x^k term multiplied by $k!$. If we take k derivatives of f, the coefficients of the power terms $1, x-a, (x-a)^2, \cdots, (x-a)^{k-1}$ all vanish. Then the term $c_k(x-a)^k$ in f becomes the term $c_k * k!$ in $f^{(k)}(x)$ by the power rule. Evaluating at $x = a$, we have $f^{(k)}(a) = c_k * k!$ and so $c_k = \frac{f^{(k)}(a)}{k!}$. Note the field characteristic is irrelevant, as dividing each coefficient of $f^{(k)}(x)$ by $k!$ gives a multiple of a binomial coefficient $\binom{n}{k}$ in the coefficient of a given power term. Thus, the expansion as in Theorem 4.1 holds for fields of any characteristic. □

With Taylor's Theorem established, we can now introduce our main theorem for this section.

Theorem 4.3. *(Hensel) Let $f(x) \in \mathbb{Z}[x]$, and suppose there is an integer $x_0 \equiv 0 \pmod{p}$. If moreover $f'(x_0) \not\equiv 0 \pmod{p}$, then for all $n \geq 1$ there is an $x_n \in \mathbb{Z}$ such that $f(x_n) \equiv 0 \pmod{p^{n+1}}$. Additionally, if we require $x_n \equiv x_0 \pmod{p}$, then x_n is unique modulo p^{n+1}. Then we may take $x_{n+1} \equiv x_n \pmod{p^{n+1}}$.*

Proof. We paraphrase the proof given in [1]. Since $f(x) \in \mathbb{Q}[x]$, we may use Theorem 4.1 and write f as a Taylor expansion. We then proceed by induction. The base case $n = 0$ is true by hypothesis. Now assume we have the result for $n = m - 1$, where $m \in \mathbb{Z}^+$. We now show that the result holds for $n = m$. Since we require $x_m \equiv x_0 \pmod{p}$ and $x_{n+1} \equiv x_n \pmod{p^{n+1}}$, we write $x_m = x_{m-1} + p^m t$ for some integer t. We then have

$$f(x) = \sum_{k=0}^{deg(f)} \frac{f^{(k)}(x_{m-1})}{k!} p^{mk} t^k \equiv f(x_{m-1}) + f'(x_{m-1}) p^m \pmod{p^{m+1}}$$

since $2m \geq m + 1$. Note that each $f^{(k)}(x_{m-1})/k!$ term is actually an integer as $k!$ yields a multiple of a binomial coefficient in the coefficient of each power term in $f^{(k)}(x)/k!$. Then,

$$f(x_{m-1}) + f'(x_{m-1}) p^m t \equiv 0 \pmod{p^{m+1}} \implies t \equiv \frac{-f(x_{m-1})/p^m}{f'(x_{m-1})} \pmod{p^{m+1}}.$$

Note that the numerator is an integer since $p^m \mid f(x_{m-1})$ by inductive hypothesis. Since $f'(x_{m-1}) \equiv \pmod{p}$, we have $f'(x_{m-1}) \not\equiv 0 \pmod{p}$ and so division by $f'(x_{m-1})$ modulo p^{m+1} is defined. Thus, such a value of t exists, and furthermore it is unique. Theorem 4.3 has now been proven. □

Notice how this value of t yields the value $x_m \equiv x_{m-1} - \frac{f(x_{m-1})}{f'(x_{m-1})} \pmod{p^{m+1}}$. With initial approximation x_{m-1}, notice how this value is the approximation of the root of f by Newton's Method! This is not a coincidence, and its explanation relies on a completely new and somewhat odd number system: the p-adic numbers.

5. p-adic Numbers

We thus pause on our discussion of solutions to polynomials to introduce a new and useful number system (as we described in §4): the p-adic numbers, denoted $\mathbb{Q}_p$. The elements of

$\mathbb{Q}_p$ are numbers of the form

$$\sum_{i\in\mathbb{Z}} a_i p^i,$$

where the $a_i \in \mathbb{Z}/p\mathbb{Z}$. What is intriguing about this set of numbers is that it uses a different notion of "distance," known as the "p-adic metric," defined as $\left|\frac{a}{b}\right|_p = p^{-\mathrm{val}_p(\frac{a}{b})}$, $a, b \in \mathbb{Z}$. We further define $\mathrm{val}_p(\frac{a}{b}) = \mathrm{val}_p(a) - \mathrm{val}_p(b)$. To construct $|\cdot|_p$ as an absolute value, we define $|0|_p = 0$. We define $\mathbb{Z}_p$ to be a subset of $\mathbb{Q}_p$ with p-adic absolute value less than or equal to 1. More concretely, elements in $\mathbb{Z}_p$ are of the form

$$\sum_{i=0,i\in\mathbb{Z}}^{\infty} a_i p^i \tag{5.1}$$

This number system is seemingly counterintuitive: informally, the p-adic norm of a number gets smaller as that number "increases" in divisibility by p, its value decreases in $\mathbb{Q}_p$ and vice versa. We will see in §6 that this number system is useful in our study of rational solutions to polynomials with rational coefficients and makes the applications of Theorem 4.3 apparent. Thus it is important that we first discuss the motivation of the construction of the p-adic numbers, which centers around this different notion of "distance" in the p-adics.

In a set of numbers there are choices as to how we define distance between two points. Traditionally, in high school math classes we use the regular absolute value, defined as:

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases} \tag{5.2}$$

This absolute value is a special case of a general notion known as a metric, which is how distance is defined between two elements of a set S, denoted $d(x, y)$, where $x, y \in S$. Formally, a metric is a map $d : S \times S \to [0, +\infty)$ and must satisfy the following properties (5.3):

(1) $d(x, y) \geq 0$
(2) $d(x, y) \geq 0 = 0 \iff x = y$
(3) $d(x, y) = d(y, x)$
(4) $d(x, z) \leq d(x, y) + d(y, z)$

The trivial metric on a set S is defined to be:

$$d(x,y) = \begin{cases} 0 & x = y \\ 1 & x \neq y \end{cases}$$

Since we are primarily interested with rational solutions to polynomials with rational coefficients, we let $S = \mathbb{Q}$. By a well-known theorem by Ostrowski, there are only 2 classes of non-trivial absolute values: the first is (5.2), and the second is the p-adic absolute value.

We now turn to an immediate application of the p-adic numbers, which is the explanation of the occurrence of Newton's Method in the proof of Theorem 4.3. Consider a polynomial in one variable with rational coefficients $f(x)$. Theorem 4.3 tells us that if there exists an integer solution x to $f(x) \equiv 0 \pmod{p}$ such that $f'(x) \not\equiv 0 \pmod{p}$, then we may find solutions modulo higher powers of p. Consider the power expansion of x as in (5.1). Suppose there exists $x = x_0$ such that the conditions of Theorem 4.3 are satisfied. Then, using the notation of Theorem 4.3, we set $a_i = x_i$ and we obtain an infinite power series expansion for x, and this power series converges in $\mathbb{Q}_p$ by the p-adic absolute value. Thus, Theorem 4.3 is actually giving us a method to better approximate solutions to f in $\mathbb{Q}_p$! It is intuitively natural, then, that some method of root-approximation would be found in the proof of Theorem 4.3, and in this case, it happens to be Newton's Method. Furthermore, Theorem 4.3 gives us a direct way to find $\mathbb{Z}_p$ solutions to f! In the next section we analyze how existence of rational solutions to rational polynomials can be derived from finding solutions in $\mathbb{Q}_p$.

6. The Hasse Principle

The Hasse Principle is of great importance in mathematics. It is not a generalized theorem, but more of a philosophy to be used when finding rational solutions to rational polynomials. For the purpose of this section, we call $\mathbb{Q}$ a "global field" and $\mathbb{Q}_p$ and $\mathbb{R}$ "local fields." The Hasse Principle says that for some polynomials we can formulate a "local-to-global principle" that allows us to solve a polynomial in each local field to solve it in the global field.

We begin by analyzing the simple equation $x^r = a$ and formulate a principle that allows us to solve this equation in $\mathbb{Q}$. We have the following theorem:

Theorem 6.1. *For any positive integer r, the equation $x^r = a$ has a rational solution if and only if $x^r = a$ is solvable in $\mathbb{R}$ and $\mathbb{Q}_p$.*

Proof. We first show the only if direction. If $x^r = a$ is solvable in $\mathbb{Q}$, then it is clearly solvable in $\mathbb{R}$ since $\mathbb{Q} \subset \mathbb{R}$. Every rational number has a power series representation with base p, so this solution is an element of each $\mathbb{Q}_p$.

Now assume that $x^r = a$ is solvable in $\mathbb{R}$ and each $\mathbb{Q}_p$. The latter implies that $r \mid val_p(a)$, and so every prime in a appears as an nth power. Thus, $a = \pm b^n$ for some rational number b. If r is odd we let $x = b$ if the sign is positive and $x = -b$ if the sign is negative. If r is even, then a is forced to be positive since $x^r = a$ is solvable in $\mathbb{R}$. Here we may set $x = b$. □

The Hasse Principle extends its usefulness to polynomials in more than 1 variable. One of the most famous examples is the following theorem due to Hasse and Minkoswki:

Theorem 6.2. *(Hasse-Minkowski) Let $f(X_1, X_2, \cdots, X_n)$ be a quadratic form with rational coefficients. Then,*

(1) *For $c \in \mathbb{Q}^\times$, the polynomial $f(X_1, X_2, ..., X_n) - c$ has a solution in $\mathbb{Q}$ if and only if it has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$.*
(2) *f has a solution in $\mathbb{Q}$ other than $(X_1, X_2, \cdots, X_n) = (0, 0, ..., 0)$ if and only if it has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ that is not $(X_1, X_2, ..., X_n) = (0, 0, ..., 0)$.*

Moreover, when $n \geq 2$, solvability in $\mathbb{Q}_p$ is automatic unless $p = 2$ or some coefficient of f is not in $\mathbb{Z}_p^\times$.

Proof. See [3, §6]. □

We end this section with an example of an application of Theorem 6.2, a discussion of which can also be found in [2].

Example 6.3. Let $f(x, y) = 2x^2 + 7y^2 - 1$. Theorem 6.2 tells us that f has a rational solution if and only if f is solvable in $\mathbb{R}$, $\mathbb{Q}_2$, and $\mathbb{Q}_7$. Thus we only need to check if f has a solution in these local fields. f clearly is solvable in $\mathbb{R}$ (i.e., $(x, y) = (0, \sqrt{1/7})$). We claim that for $p = 2, 7$, f has a $\mathbb{Z}_p$ solution, and hence a $\mathbb{Q}_p$ solution. For $p = 2$ we have $y^2 = -1/7$. It remains to show that $-1/7$ is a square in $\mathbb{Z}_2$. We require the following lemma:

Lemma 6.4. *a is a square in $\mathbb{Z}_2$ if $a \equiv -1 \pmod 8$.*

Proof. We claim there exists some integer x such that $(1 + 2x)^2 = 8k - 1$. This reduces to $x^2 + x - 2 = 0$. The congruence $x^2 + x - 2b \equiv \pmod 2$ has solution $x = 0$. The derivative evaluated here equals 1, and hence we may apply Theorem 4.3 and the discussion at the end of §4 to conclude that $8k + 1$ is a square in $\mathbb{Z}_2$. □

Note that $7^{-1} \equiv -1 \pmod 8$ since $7(-1) \equiv -7 \pmod 8 \implies 7(-1) \equiv 1 \pmod 8$. Thus, $-1/7 \equiv (-1)(7^{-1}) \pmod 8 \implies -1/7 \equiv 1 \pmod 8$. Then Lemma 6.3 allows us to conclude that $-1/7$ is a square in $\mathbb{Z}_2$, and so f is solvable in $\mathbb{Z}_2$.

For $p = 7$, we have $f \equiv 0 \pmod 7 \implies 2x^2 \equiv 1 \pmod 7 \implies 8x^2 \equiv 4 \pmod 7 \implies x^2 \equiv \pm 2 \pmod 7$. We may take the positive sign and use Proposition 3.1 and the discussions in §4 to conclude there exists a solution to f in $\mathbb{Z}_7$.

Since f is solvable for all required cases, we apply Theorem 6.2 to conclude that f has a solution in the rational numbers. We may verify this directly by noting that $(x, y) = (1/3, 1/3)$ is a solves f in $\mathbb{Q}$.

7. Conclusion

In order for the theory developed in this report to be useful, it must be true that finding solutions in the p-adic numbers is easier than finding solutions in the rational numbers. It is intuitive, however, that this should generally be the case. First, the history of finding rational solutions to rational polynomials dates back centuries. If finding such solutions were simple, mathematicians would have already discovered an argument for existence centuries ago. Second, we may take Example 6.3. There are no obvious rational solutions to f.

Finding rational solutions by hand would simply be a matter of guess and check. One might try using the number system $\mathbb{Z}/n\mathbb{Z}$ to try to restrict the number of solutions, but even this method has no certainty of success.

However, §6 shows that for some polynomials, there is no need to use $\mathbb{Z}/n\mathbb{Z}$ to restrict the possible rational solutions to a rational polynomial f. Rather, letting n be prime, we simply solve the congruence $f \equiv 0 \pmod{p}$ for a limited number of p and apply Theorem 4.3 to obtain a $\mathbb{Q}_p$ solution!

To close, we expand on one large gap left behind by Hasse. Theorem 6.2 states that we may apply a "local-to-global principle" to quadratic forms f (i.e., $\deg(f) = 2$). As we increase the degree of f, the Hasse Principle starts to break down. One of the most famous examples is due to Selmer: consider the polynomial $f(X, Y, Z) = 3X^3 + 4Y^3 + 5Z^3$. One can show it has a p-adic solution for all primes p, but it does not have any rational solution other than the trivial solution $(X, Y, Z) = (0, 0, 0)$.

Such counterexamples should not detract from the utility of the notions provided by the Hasse Principle, though. The Hasse Principle is, by nature, imperfect. But its utility lies in the potential for reduction in the difficulty of finding rational solutions to rational polynomials. Indeed, there is still much more work to be done in this rich field of study, which is what makes it all the more exciting.

References

[1] P. Corn, P. Roy, A. Purswani, A. Roopesh, M. Jain, J. Khim, *Hensel's Lemma*. Brilliant.org, 2018.

[2] K. Conrad, *The Local-Global Principle*. Keith Conrad, 2016.

[3] H. Cohen, *Number Theory I*, GTM 239 Springer, 2010.

[4] E. Weisstein, *Field Axioms*. Wolfram MathWorld, 2018.