Representation by Quadratic Forms Over Field of the P-adic Numbers

[1]Ms. Chetna, [2]Dr. Hardeep Singh
[1]Assistant Professor, Dept. of Mathematics, M.M. Modi College, Patiala, Punjab, India
[2]Professor and Head, Dept. of Mathematics, Government Mahindra College, Patiala, Punjab, India

Abstract
In this paper, we attempt to find the solution of the quadratic forms over local field Q_p and then we give the representation of elements by these quadratic forms in Q_p. This paper provides the extension of the concept of congruence modulo p-adic integers and p-adic numbers and solves them. Further, we link it with congruence on the integers modulo powers of prime numbers. The properties of the p-adic numbers are also discussed and most importantly an attempt is being made to re-formulate the Hensal Lemma with a different approach.

Keywords
Quadratic Forms, Congruence, P-adic Number, P-adic Integer and Hensal Lemma

I. Introduction

In the present paper, firstly we define the congruence for p-adic numbers. Then we establish the association between solution of the congruence polynomial modulo p^n for all n and solution of the p-adic numbers. Finally, we discuss the lemma given by Hensel with the new approach. For elementary results and definitions we are following the work of Burton [2], Alladi, Bhargava, Savitt [1] and Gerstein [4].

II. Definition

Let x, y, $z \in Q_p$, z is a non-zero element. Then we can say that x is congruent to y modulo z if z divides (x-y) for each element in Q_p. Also $z = p^m \epsilon$ where ϵ a unit element and $m \in Z$ is the unique representation such that we have $x \equiv y (\text{mod} p^m)$. Therefore, we can focus our attention on congruence modulo p^m. It should be noted that $x \equiv y (\text{mod} p\hat{}m)$ is also equivalent to $|x-y|_p \leq p^{-m}$.

Further, there are two ways regarding this over p-norm. First is usually when we consider $x \equiv y (\text{mod} p^m)$, where $x,y,z \in Q_p$ and then formulate that x-y is divisible by z. Clearly, this is a special case of the above definition for the p-adic integers and second is that when we consider in general that each ring is congruent. The p-adic numbers considered as ring is congruent to a non-zero element. Thus we observe that the necessary and sufficient condition for the p-adic integer a to be a unity in O_p is obviously that $a \not\equiv 0 (\text{mod} p)$ and thus the same condition is in the case of congruence of p-adic integers. So the condition is similar for an integer m on the inverse which has to be a unit in the ring Z_n. Now we are going to discuss the existence of solution of Z and Q. Parimala, R. and Suresh, V [8].

Solution of Z in O_p and Q in Q_p

Result 1.1: Each p-adic number is congruent to an integer modulo p^n

Proof: - Let x is a p-adic number which is completely determined by (a_n). On taking the p-adic expansion of x it is clear from the first element a_{n-1} that the elements of the sequence are congruent to the p-adic integer modulo p^n. We show that $x \equiv a_{n-1} (\text{mod} p^n)$.

For this we prove that the sequence (a_n)-a_{n-1} approaches to the p-adic number $x-a_{n-1}$.

Thus it is sufficient to prove that p^n is a divisor of this p-adic number. We have
$a_{n-1} \equiv a_k (\text{mod} p^{k-1})$, (k=0,1……,n-1)

Thus the required result is clear from the condition of the sequence of integers which determines the p-adic number. Further, it is also clear that by the definition of the Q_p as a fraction field in the field O_p in which Q is everywhere dense in Q_p and also for $p=\infty$. In general, we find congruence of integers α and β modulo γ in Z which is not the same as the congruence of those integers in O_p . It is clear that if α and β are congruent in Z then they are congruent in O_p. Even if we are restricted to congruence modulo p^n then it remains same. From all this it is clear that the only thing which is not allowed in both cases is that the prime p gives a negative exponent in $(a-b)/p^n$. This formally follows by the following proposition.

Result 1.2: Two integers are congruent to modulo p^n in the ring O_p if and only if they are congruent to modulo p^n in the ring Z

Proof:- Let a and b are two integers. We assume $a \neq b$ otherwise the assertion is trivial.
We can write

$$a-b = p^m \alpha, \alpha \not\equiv 0 (\text{mod} p) \qquad (1.1)$$

The congruence $a \equiv b (\text{mod} p^n)$ in the ring Z is equivalent to the condition $m \geq n$. This condition is equivalent to $\text{ord}_p (a-b) \geq \text{ord}_p (p^n)$. Since p^n divides a-b in O_p and hence this is equivalent to $a \equiv b (\text{mod} p^n)$ in the ring O_p.

Result 1.3: Let P be a finite set of prime numbers. Let $z_p \in O_p$ for each $p \in P$. Then for every $\epsilon > 0$ there exists an integer $z \in Z$ such that for all $p \in P$, we have

$$|z-z_p|_p < \epsilon$$

In other words we can say that $z \equiv z_p (\text{mod} p^n)$

Proof: - Consider $n \in N$ such that $p^{-n} < \epsilon$. Because of existence of the theorem 1.1 there exist $z'_p \in Z$ such that
$z_p \equiv z'_p (\text{mod} p^n)$

Then by the Chinese remainder theorem, there exist an integer $z \in Z$ such that

$$z_p \equiv z'_p (\text{mod} p^n)$$

Thus $|z-z_p|_p < p^{-n} < \epsilon$.

Result 1.4: Let P is the finite set of prime numbers say p, where p can also be infinite. Let $\alpha^p \in Q_p$ for every $p \in P$. Then for each $\epsilon > 0$ there exist an integer $\alpha \in Q$ such that for all $p \in P$, we have

$$|\alpha-\alpha_p|_p < \epsilon$$

Proof: - Consider P' be the finite collection of P. Let n(p) is a natural number for each p∈P', we have $p^{n(p)}$ $a_p \in O_p$. Consider $h=\prod_{p\in P^*} P^{n(p)}$ and for all p∈P we have $z_p=ha_p$. Then there exist $z_p \in O_p$ for all p∈P'.

Let us suppose that ∈>0 and consider $\eta=|h|_p \in$. Thus there is an integer z such that

for all $p^{P'}$.

If we take P'=P for ∞∉P, then we can see that

$$\alpha = z/h$$

Now we consider the result other way round. Suppose ∞∈P . We will consider z=z' so that $|z'-z_p|_p<\eta$, for all p∈P, also for p =∞ . We again find that α=z/h.

We must keep that $|z'-z_p|_p<\eta$ for p∈P' and we ensure that $z' \equiv z (\mathrm{mod} p^{m(p)})$ where m(p) is so large such that $p^{-m(p)}<\in$. So take these m(p)≥1, and therefore we get

$$z'=z+rA$$

Where $A=\prod_{p\in P^*} p^{m(p)}$ and an appropriate value of r. These r may be a rational number but we should not take the negative powers of p in its decomposition so that $z'-z/p^{m(p)}$ is in O_p. Thus we have

$|z'-z_\infty|_\infty=|z+rA-z_\infty|_\infty<\eta$

There are other primes than that of P, because there are infinite primes. We can therefore assume a strictly positive integer B relatively prime with A, we choose these values in such a way so that A/B<η. It is clear that we can choose a proper integer t so that r = t/B and finally we get the required result.

Congruencies in O_p

In the previous Section the relationship between p-adic numbers and congruencies was already clear. By considering the p-adic expansion, we find that from the solubility of a polynomial in the p-adic integers we can find the solution of the congruence modulo p^n for all n. This section also proves the other way round. This fact has already been mentioned in the introduction and is important for our main problem.

Theorem 1.5:- Let $F(\alpha_1,\ldots\ldots,\alpha_n)$ is a polynomial with coefficient considered over the field of integers. The congruence

$$F(\alpha_1,\ldots\ldots,\alpha_n) \equiv 0 (\mathrm{mod} p^k) \quad (1.2)$$

has a solution in Z for all k≥1 if and only if $F(\alpha_1,\ldots\ldots,\alpha_n)$ has a solution in the field of p-adic numbers.

Proof:- Let $(a_1,\ldots\ldots,a_n)$ is a p-adic integral solution of the form F. From (1.1) we know that there are integers such that for each k, we have

$a_1 \equiv \alpha_1^k (\mathrm{mod} p^k),\ldots\ldots,a_n \equiv \alpha_n^k (\mathrm{mod} p^k)$

By the elementary modulo property Shimura [9], we have

$F(\alpha_1^k,\ldots\ldots,\alpha_n^k) \equiv F(a_1,\ldots\ldots,a_n) \equiv 0 (\mathrm{mod} p^k)$

Thus $(\alpha_1^k,\ldots\ldots,\alpha_n^k)$ is a solution to the congruence (1.2).

Now we prove the result conversely.

Suppose that (1.2) has the solution $(\alpha_1^k,\ldots\ldots,\alpha_{nk})$ for each k and thus for all integers α_i^k. Then by Parimala, R [7] there exist a p-adic convergent subsequence $(\alpha_1^{(ki)})_i$ of the sequence (α_1^k) where (k_i) is a strictly increasing sequence of natural numbers. Then again there exists the convergent subsequence of the sequence $(\alpha_2^{(ki)})$. On repeating the process n times, we obtain a strictly increasing sequence (l_m) of integers such that for all i the p- adic sequence $(\alpha_i^{(lm)})_m$ is convergent which implies that the limit exists. Then we set

$$a_i = \lim_m \alpha_i^{l_m}$$

Now we show that $(a_1,\ldots\ldots,a_n)$ is a solution for F in the field of p-adic integers. Since the polynomial $F(\alpha_1^k,\ldots\ldots,\alpha_n^k)$ is a continuous function. Therefore we have

$$F(a_1,\ldots\ldots\ldots,a_n) = \lim_m F(\alpha_1^{l_m},\ldots\ldots\ldots,\alpha_m^{l_m})$$

This is also true from the fact that

$$F(\alpha_1^{(l_m)},\ldots\ldots\ldots,\alpha_n^{(l_m)}) \equiv 0 (mod p^{(l_m)})$$

Thus for increasing m the polynomial $F(\alpha_1^{(l_m)},\ldots\ldots\ldots,\alpha_n^{(l_m)})$ approaches to zero with respect to the p-norm and hence the limit is zero.

We have a similar argument for homogeneous polynomial forms.

Theorem 1.6:- Let $F(\alpha_1,\ldots\ldots,\alpha_n)$ is a form with coefficient considered over the field of integers. The congruence

$$F(\alpha_1,\ldots\ldots,\alpha_n) \equiv 0 (\mathrm{mod} p^k) \quad (1.3)$$

for all k≥1 has an integral solution where not all terms are divisible by p if and only if $F(\alpha_1,\ldots\ldots,\alpha_n)$ has a non-zero solution in O_p

Proof:- Let us assume that F has a non-zero solution in O_p. Suppose that $(a'_1,\ldots\ldots,a'_n)$ is one of the solutions. Let $m=\min(\mathrm{ord}_p(a'_1),\ldots\ldots,\mathrm{ord}_p(a'.))$. Then all elements a'_i can be written in the form

$$a'_i = p^m a_i$$

where a_i are the p-adic integers.

Thus it is clear that $(a_1,\ldots\ldots,a_n)$ also has a non-zero solution in O_p for F which satisfies the additional condition that a_i say a_{i0} is not divisible by p. The proof is now corresponding to that of the above theorem. Therefore we have the result for each element k where $\alpha_{i0}^{(k)}$ is not divisible by p.

Now we prove the result conversely. Suppose that (1.3) has a solution $(\alpha_1^k,\ldots\ldots,\alpha_n^k)$ for each k which satisfies the given condition. Because there are only a finite α_i with the index i_0 for which there are infinitely many values of m such that $\alpha_{i0}^{(m)}$ is not divisible by p. These values form a sequence (m_i). The proof regarding this argument can now be taken over with the only modification that the p-adic convergent sequence $(\alpha_1^{(ki)})_i$ now has subsequence of $(\alpha_1^{(mi)})_i$. If a_i can be defined as the limit a_{i0} which cannot be divisible by p then a_{i0} is not equal to zero, which follows the result.

From above it is observed that the condition of getting an integral solution where not all terms are divisible by p actually has a primitive solution. Thus it is clear that in both the statements the coefficient considered for F may also be the p-adic number. Now after the link with congruence on the integers modulo powers of prime numbers is laid down further we are going to reformulate the Hensel lemma with different approach.

The Hensel Lemma

From the above statements, it is clear that we can solve a polynomial over the p-adic number if we can solve an infinite series of congruencies. Now, we formulate Hensel Lemma that gives us simple conditions in certain cases. This lemma has many different formulations, versions and there are different ways to prove it for example Conrad [3], Herwig [5] and Kuhlmann [6] have proved Lemma in their own way and that has also motivated the present research to reformulate Lemma again. Moreover, in

the past researches the Lemma has been proved without using the p-adic numbers but in the present study an attempt has been made to reformulate the Hensel Lemma with p-adic numbers.

Theorem 1.7:- Let $F(\alpha_1,\ldots\ldots,\alpha_n)$ is a polynomial with coefficient as p- adic integers. Let θ is a natural number. If $\varphi_1,\ldots\ldots,\varphi_n$ are the p-adic integers for any i,$(1\leq i\leq n)$ we have

$$F(\varphi_1,\ldots\ldots\ldots,\varphi_n)\equiv 0\left(modp^{2\theta+1)}\right),$$

$$\frac{\partial F}{\partial x_i}((\varphi_1,\ldots\ldots\ldots,\varphi_n)\equiv 0\left(modp^{\theta}\right),$$

$$\frac{\partial F}{\partial x_i}((\varphi_1,\ldots\ldots\ldots,\varphi_n)\not\equiv 0\left(modp^{\theta+1}\right),$$

then there exist p- adic integers $\beta_1,\ldots\ldots,\beta_n$ such that

$$F(\beta_1,\ldots\ldots,\beta_n)=0$$

and

$\beta_1\equiv\varphi_1\ (modp^{\theta+1}),\ldots\ldots,\beta_n\equiv\varphi_n\ (modp^{\theta+1})$

Proof: - Let us consider the polynomial

$f(\alpha)=F(\varphi_1,\ldots\ldots,\varphi_{i-1},\alpha,\varphi_{i+1},\ldots\ldots,\varphi_n)$

In order to prove the theorem it is sufficient to obtain a p-adic integer a for which $f(a)=0$ and $a\equiv\varphi_i\ (modp^{\theta+1})$

Set $\varphi_i=\varphi$ and construct a sequence

$$a_0,a_1,a_2,\ldots\ldots \qquad (1.4)$$

of p-adic integers congruent to $\varphi(modp^{\theta+1})$ so that we have

$$f(a_m)\equiv 0(modp^{2\theta+1+m)}),\forall\ m\geq 0 \qquad (1.5)$$

For m=0 we choose $a_0=\varphi$ and let us assume that a_i where $i<m,\forall$ $m\geq 1$ represent the above sequence. Now we will find a_m.

Write the polynomial $f(\alpha)$ in powers of $(\alpha-a_{m-1})$ as

$$f(\alpha)=b_0+b_1\ (\alpha-a_{m-1})+b_2\ (\alpha-a_{m-1})^2+\cdots \qquad (b_i\in O_p)$$

then $b_0=f(a_{m-1})=p^{2\theta+m}\ A$ where A is a p-adic number.

The condition follows from the statement because $a\_(m-1)\equiv\varphi(modp^{\theta+1})$ for which we have

$$b_1=f'\ (a_{m-1})=p^{\theta}\ B$$

where B is not divisible by p in O_p. Now if we suppose $\alpha=a_{m-1}+\delta p^{m+\theta},(\delta\in O_p)$ then we obtain the following

$f(a_{m-1})+\delta p^{m+\theta})=p^{2\theta+m}(A+\delta B)+b_2\ p^{2\theta+2m}\ \delta^2+\cdots$

Let us consider $\delta=\delta_0\in O_p$ so that $A+B\delta_0\equiv 0(modp)$. Since $B\not\equiv 0(modp)$ thus we can choose the value of δ_0 in such a way so that B has an inverse in O_p.

Since $k\theta+km\geq 2\theta+1+m$ for all $k\geq 2$ where

$f(a_{m-1})+\delta_0\ p^{m+\theta})\equiv 0(modp^{2\theta+1+m})$

Now we set $a_m=a_{m-1}+\delta_0\ p^{m+\theta}$. Thus in order to verify that the chosen value of a_m is appropriate we have to prove that

$$a_m\equiv\varphi(modp^{\theta+1})$$

This result follows because when $m+\theta\geq\theta+1$, we have $a_m\equiv a_{m-1}$ $(modp^{\theta+1})$.

By Gerstein [4] we have $|a_m-a_{m-1}\ |p\leq p^{-m-\theta}$, thus the sequence (1.4) converges to the limit say a therefore

$$a\equiv\varphi(modp^{\theta+1})$$

From (1.5) it follows that $\lim f(a_m)=0$. Since f being a polynomial is continuous which implies that $\lim f(a_m)=f(a)$.

Thus, $f(a)=0$, this follows the proof.

It should be noted that the condition that a partial derivative may not be congruent to zero modulo to $p^{\theta+1}$ implies that for all i it may not be congruent to zero modulo $p^{\theta+1}$. Thus the congruence $F(\varphi_1,\ldots\ldots,\varphi_n)\equiv 0(modp^{2\theta+1})$ does not has zero solution. Further, since $\beta_i\equiv\varphi_i\ (modp^{\theta+1})$ which also implies that for all $\beta_1,\ldots\ldots,\beta_n$ form F has a non-zero solution in O_p. Thus for quadratic forms this is important that the quadratic form has a solution or represents zero if there is a non-zero solution.

Since the above formulation of Hensel lemma leads to the following result which follows immediately by taking θ=0.

Corollary 1.8:- Let $F(\alpha_1,\ldots\ldots,\alpha_n)$ is a polynomial with coefficient in O_p. Let $\varphi_1,\ldots\ldots,\varphi_n$ are p-adic integers such that for any i,$(1\leq i\leq n)$ we have

$F(\varphi_1,\ldots\ldots,\varphi_n)\equiv 0(modp)$,

$\partial F/(\partial x_i)\ (\varphi_1,\ldots\ldots,\varphi_n)\not\equiv 0(modp)$,

then there exist p- adic integers $\beta_1,\ldots\ldots,\beta_n$ such that

$F(\beta_1,\ldots\ldots,\beta_n)=0$

and

$\beta_1\equiv\varphi_1\ (modp),\ldots\ldots,\beta_n\equiv\varphi_n\ (modp)$

Thus, a solution $(c_1,\ldots\ldots,c_n)$ of the congruence $F(\alpha_1,\ldots\ldots,\alpha_n)\equiv 0(modp)$ can be extended to a solution of the polynomial $F(\alpha_1,\ldots\ldots,\alpha_n)$ in the ring O_p provided that there exists i such that

$\partial F/(\partial x_i)((\varphi_1,\ldots\ldots,\varphi_n)\not\equiv 0(modp)$

Now we give a different formulation for the Hensel lemma which equivalent to the previous formulation.

Theorem 1.9:- Let $F(\alpha_1,\ldots\ldots,\alpha_n)$ is a polynomial with coefficient in O_p. Let $\varphi_1,\ldots\ldots,\varphi_n$ are p-adic integers such that for any i,$(1\leq i\leq n)$ we have

$|F((\varphi_1,\ldots\ldots,\varphi_n)\ |_p<|F'_{xi}\ (\varphi_1,\ldots\ldots,\varphi_n)\ |_p^2$

then there exist p-adic integers $\beta_1,\ldots\ldots,\beta_n$ such that

$F(\beta_1,\ldots\ldots,\beta_n)=0$

and

$\beta_1\equiv\varphi_1\ (modp^{\theta+1}),\ldots\ldots,\beta_n\equiv\varphi_n\ (modp^{\theta+1})$

Proof: - Because of the two congruence conditions on the evaluation of F' in the previous formulation, we have that for certain $\varphi_1,\ldots\ldots,\varphi_n$ where the variable θ is fixed. However θ should be arbitrary. Therefore, it is sufficient to prove the following.

Let $F(\alpha_1,\ldots\ldots,\alpha_n)$ is a polynomial with coefficient in O_p. Let $\varphi_1,\ldots\ldots,\varphi_n$ are the p-adic integers and for any i,$(1\leq i\leq n)$ the following result holds

$|F((\varphi_1,\ldots\ldots,\varphi_n)\ |_p<|F'_{xi}\ (\varphi_1,\ldots\ldots,\varphi_n)\ |_p^2$

if and only if

$F(\varphi_1,\ldots\ldots,\varphi_n)\equiv 0(modp^{2\theta+1)})$,

where θ is the natural number such that

$$\frac{\partial F}{\partial x_i}(\varphi_1,\ldots\ldots\ldots,\varphi_n)\equiv 0\left(modp^{\theta}\right),$$

$$\frac{\partial F}{\partial x_i}(\varphi_1,\ldots\ldots\ldots,\varphi_n)\not\equiv 0\left(modp^{\theta+1}\right),$$

Proof:- Since θ is the natural number so therefore we have

$$\left|\frac{\partial F}{\partial x_i}(\varphi_1, \dots\dots\dots, \varphi_n)\right|_p = p^{-\theta}$$

Thus

$$|F(\varphi_1,\dots\dots\dots,\varphi_n)|p<|F'_{xi})\ (\varphi_1,\dots\dots\dots,\varphi_n)|_p{}^2$$

if and only if

$$|F(\varphi_1,\dots\dots\dots,\varphi_n)|p\leq p^{-2\theta-1}$$

if and only if

$$F(\varphi_1,\dots\dots\dots,\varphi_n) \equiv 0(\mathrm{mod} p^{2\theta+1)})$$

Hence we get the desired result.

References

[1] Alladi Krishnaswami, Bhargava Manjul, Savitt David; (Editors),"Quadratic and Higher Degree Forms (Developments in Mathematics)", Springer, 2013.

[2] Burton David M.,"Elementary Number Theory", 6th Ed., Tata McGraw-Hill, 2010.

[3] Conrad Keith, Hensel's Lemma, [Online] Available: http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/hensel.pdf.

[4] Gerstein Larry,"Basic Quadratic Forms", Graduate Studies in Mathematics, Vol. 90, American Mathematical Society, 2008.

[5] Herwig T.,"The p-adic Completion of Q and Hensel's Lemma", [Online] Available: http://www.math.uchicago.edu/ may/VIGRE/VIGRE2011/REUPapers/Herwig.pdf

[6] Kuhlmann, Franz-Viktor,"Maps on Ultrametric Spaces, Hensel's Lemma, and Differential Equations over Valued Fields", Communications in Algebra, 39, pp. 1730-1776, 2011.

[7] Parimala, R,"A Hasse Principle for Quadratic Forms over Function Fields, Bulletin of the American Mathematical Society", Vol. 51, No. 3, (2014), pp. 447–461. [Online] Available: http://www.ams.org/journals/bull/2014-51-03/S0273-0979-2014-01443-0/S0273-0979-2014-01443-0.pdf

[8] Parimala, R., Suresh, V.,"Isotropy of quadratic forms over function fields in one variable over p-adic fields", Publ. de I.H.E.S. 88, pp. 129-150, 1998.

[9] Shimura Goro,"Arithmetic of quadratic forms", Springer-Verlag New York, Inc. 2010.

Ms. Chetna, M.Sc (Mathematics), M.Phil, is presently working as Assistant Professor in the Department of Mathematics at M.M. Modi College, Patiala, Punjab. She has more than thirteen years of rich experience of teaching and research. She has attended many national and international conferences and seminars. She has One book and Five research papers published to her credit. Currently, she is at the completion stage of her Doctoral Programme which is centrally focused on finding the advanced solutions of Quadratic Forms. She has also done pioneering work by proving the Hensel's Lemma with a different method.