A SURVEY OF SOME CONGRUENCES MODULO PRIME AND PRIME POWERS WITH SPECIAL REFERENCES TO GENERALISATIONS OF FERMAT'S LITTLE THEOREM

SHAILANSTAR KHONGSIT
DEPARTMENT OF MATHEMATICS
NORTH-EASTERN HILL UNIVERSITY

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT OF THE DEGREE OF

MASTER OF PHILOSOPHY

TO

North-Eastern Hill University
Shillong
October, 2003

Supervisor

maths

NEHU LIBRARY
Acc. No. 103327
28-3-05

CERTIFICATE

I certify that the dissertation entitled 'A SURVEY OF SOME CONGRUENCES MODULO PRIME AND PRIME POWERS WITH SPECIAL REFERENCES TO GENERALISATIONS OF FERMAT' S LITTLE THEOREM' submitted by Mr. Shailanstar. Khongsit in partial fulfilment of the requirements for the degree of Master of Philosophy is the outcome of a study undertaken by the candidate.

I certify that the sources from which ideas have been borrowed have been duly referred to.

The material in this dissertation has not been presented for the award of a degree in any university before.

This dissertation may be placed before the examiners for evaluation and necessary formalities. I certify that this dissertation is worthy of consideration by the examiners.

Promode Kumar Saikia
Supervisor
Department of Mathematics
North-Eastern Hill University
Shillong

Shillong
October 15, 2003

DECLARATION

I, Shailanstar Khongsit, hereby declare that the subject matter in this dissertation is the record of work done by me, that the contents of this dissertation did not form basis of the award of any previous degree to me or to the best of my knowledge to anybody else, and that the dissertation has not been submitted by me for any research degree in any other university/institute.

This dissertation is being submitted to the North-Eastern Hill University for the degree of Master of Philosophy in Mathematics.

MB Rege

Signature of the Head

Signature of the Supervisor

S. Khongsit

Signature of the Candidate

ACKNOWLEDGEMENT

This work was carried out under the guidance of Dr. P. K. Saikia. I wish to thank him for his guidance and support during the preparation of the dissertation.

Thanks are also due to Prof. H. K. Mukherjee, Prof. S. S. Khare, Prof. M. B. Rege and Dr. R. P. Shukla for their guidance during the M. Phil. Coursework programme.

I would like to thank other teachers in the Department , Prof. S. K. Srivastava, Mr. S. L. Marbaniang, Dr. C. R. Mondal, Dr. A. K. Das, Ms. A. M. Buhphang , Mr. A. Tiken Singh, Ms. Sanghita Dutta and colleagues for their encouragement. I would also like to thank all the office staff for their help.

Finally, I thank all all the members of my family and my relatives for their support and for being my constant source of inspiration.

Shailanstar. Khongsit

PREFACE

Congruences are statements about general divisibility properties of integers, as well as of rationals (if properly interpreted in this case). Many proofs in number theory can be seen as extended sequences of deductions about the divisibility properties of integers. These deductions can be greatly simplified by the simple mechanism of expressing the divisibility relations as equations or what is commonly known as **congruences**. This mechanism was devised by the great mathematician Gauss, who showed that the advantage of using congruence was in the fact that they could be manipulated in accordance with the ordinary rules of algebra. The ease with which congruences can be algebraically manipulated not only speeds up calculations tremendously, but also throws up unexpected divisibility relations.

Some simple congruences, singling out essential aspects of divisibility in integers form the very basis of elementary number theory as we know it now. Among them, the congruence known as Fermat's Little Theorem (named after one of the founders of number theory, P. Fermat (1601-1665) immortalised by the famous Fermat's Last Theorem) though simple, is one of the most useful basic relations in elementary number theory. Equally important are some other elementary congruences modulo primes and prime powers. Numerous attempts have been made, and no doubt will be made in future, to generalise these congruences. For, any fruitful generalisation will bring out deeper divisibility relations.

This survey originally started as an attempt to understand some of the generalisations (though partial) of Fermat's Little Theorem. This led nat-

urally to studying various ingenious methods used to prove congruences of different types. One of the most fascinating ways of dealing with congruences is to use deep results from p-adic analysis. The work of Chowla, Dwork and Evans [5] is a prime example. Some recent work, as detailed in A.Robert's book [15] also strengthen the case for using p-adic analysis for generalising old congruences and discovering new ones.

Thus, this survey has two parts. The first part essentially covers generalisations of some basic congruences using elementary methods. This part also discusses a few little-known congruences if only to emphasise their unusual proofs. The second part starts with a brief introduction to p-adic field and analysis therein. The aim of the second part is to focus on the basic features of the p-adic methods used to prove congruences of some binomial coefficients modulo prime powers.

Now we give a chapterwise description of this survey. The first chapter begins leisurely by looking at three of the well-known elementary congruences namely Fermat's , Wilson's and Wolstenholme's. Eisenstein's famous generalisation [10,12] of Fermat's little theorem follows, which we prove by using a combinatorial identity. Next, Jothilingam's [12] extension of Eisenstein's result is discussed. Two related concepts, that of Wieferich primes and Fermat quotients are also taken up in this chapter. In the most interesting part of the survey, we use Ram Murty's formula [15] for Fermat quotient to give a nice determination of $3^{p-1} \bmod p^2$, thus generalising Eisenstein's congruence. Another feature of this chapter is the unusual collection of various generalisations of Wolstenholme's congruence. We round up the chapter by looking at some congruences and their proofs which we consider to be of interest in

our future programme.

The second chapter treats a few of the classical congruences satisfied by Bernoulli numbers. Our choice is dictated by the usefulness of such congruences in our main programme. After introducing Bernoulli numbers and their basic properties, we quickly establish Von-Staudt's Theorem and Voronoi congruences. Voronoi type sums are important for us as they are similar to sums appearing in the formula for Fermat quotients. Finally, we could not resist the temptation of discussing Chowla's neat use [4] of Von Staudt's result to establish a generalisation of Wolstenholme's congruence.

Chapter 3 is a brief discussion of the tools that we require from p-adic analysis for the study of certain congruences. Starting with the basic description of the p-adic field Q_p and its extensions $\bar{Q}_p$ and C_p, this chapter takes a quick look power series and Hensel's lemma application. We introduce p-adic gamma function and list some of its basic properties here.

The final chapter of the survey, the fourth chapter, basically examines the use of p-adic methods in solving congruences, specifically of congruences for some binomial coefficients. Here we are content in singling out the concepts from p-adic analysis that work in such situations. The first part is devoted to examine how the p-adic analogue of the mean value theorem of classical analysis is used to "estimate" and thus yield a congruence of certain binomial coefficients. The generalisation of this congruence, known as Kazandzidis congruence, however needs the additional input of p-adic gamma function. Our treatment of this part follows that of Robert [18]. The second part of this chapter discusses the celebrated paper of Chowla, Dwork and Evans [5] on the determination of certain binomial coefficient mod p^2. Their work utilises,

apart from p-adic gamma function, the Gross-Koblitz formula for evaluation of Gauss sums, and Diamond's formula [8] for values of the logarithm of the p-adic gamma function. It is interesting to note that Fermat quotient appears in the proof at a crucial point.

Contents

Chapter 1

Elementary Congruences And Their Generalisations

1.1 Introduction

In this chapter we begin by recording some well-known elementary congruences like Fermat's , Wilson's and Wolstenholme's theorems. It is followed by a discussion of Eisenstein's famous congruence of 2^{p-1} modulo p^2 which generalises Fermat's Little Theorem. P.Jothilingam's congruence of 2^{p-1} modulo p^3 follows. We then introduce Fermat quotient and give another proof of Eisenstein's congruence. Same method is used to give a beautiful congruence for 3^{p-1} modulo p^2. A related topic of Wieferich primes is touched on. We close the chapter by looking at some interesting generalisations of Wolstenholme's congruence.

1.2 Elementary Congruences

1.2.1 Theorem. *Fermat's Little Theorem : If p is an odd prime and a is an integer such that, $(a,p) = 1$, then*

$$a^{p-1} \equiv 1 \pmod{p}$$

1.2.2 Theorem. *Wilson's theorem : If p is a prime then*

$$(p-1)! \equiv -1(modp)$$

In text books and literature one comes across various proofs of these results. We have chosen to present proofs of Fermat's and Wilson's theorems which bring out the essential group-theoretic nature of these two results. For example, Fermat's theorem is a simple consequence of the fact that the multiplicative abelian group $(Z/pZ)^*$ whose elements are nonzero residue classes of integers modulo p has order $p-1$. Since in a group G having order $o(G)$, $a^{o(G)}$ is the identity of G, it follows that for any residue class $\bar{a} \in (Z/pZ)^*$, $\bar{a}^{p-1}$ is $\bar{1}$ in $(Z/pZ)^*$ where $\bar{1}$ is the identity of the group $(Z/pZ)^*$. But $\bar{a} = \bar{b}$ in $(Z/pZ)^*$ means $a \equiv b \pmod{p}$ and $\bar{a} \in (Z/pZ)^*$ if and only if $(a,p) = 1$. So we may conclude that for any $a \in Z$, p not dividing a,

$$a^{p-1} \equiv 1 \pmod{p}.$$

We can also prove Fermat's Little Theorem by induction on a. This proof depends on the fact that the binomial coefficient $\binom{p}{i}$ $(1 \leq i \leq p-1)$,

is divisible by p. Note that this divisibility property is a direct consequence of unique factorisation in Z. Now

$$(a+1)^p = a^p + 1 + \sum_{i=1}^{p-1} \binom{p}{i} \equiv a+1 \pmod{p}.$$

so that induction completes our verification.

For the second theorem, we observe that the left hand side is just the product of all the elements of the group $(Z/pZ)^*$. Now, in any finite abelian group, the product of all elements is trivially the product of all the elements of order 2. Since $(Z/pZ)^*$ is an abelian group having a unique element of order 2 namely $\overline{p-1}$, it follows that,

$$\overline{1} \cdot \overline{2} \cdots \overline{p-1} = \overline{p-1}$$

in $(Z/pZ)^*$ which implies that

$$(p-1)! \equiv -1 \pmod{p}.$$

Before discussing some more congruences that can be settled by using properties of the group $(Z/pZ)^*$, we need to extend the idea of congruences of integers to rational numbers. For integers $a, b, c, d\,(b, d \neq 0)$ and m, a positive integer with $gcd(bd, m) = 1$, define

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{m} \quad \Leftrightarrow \quad ad \equiv bc \pmod{m}.$$

This means , for example

$$\frac{a}{b} \equiv 0 \pmod{p}$$

for a prime p (p does not divide b) iff $p|a$.

Thus the congruence

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{(p-1)}\equiv 0 \pmod{p} \tag{1}$$

for any prime $p > 3$, is equivalent to the fact that the numerator of the fraction of the left hand side is divisible by p. This can be treated as a number-theoretic interpretation of the following result: The sum of the inverses of the nonzero elements of the field Z/pZ is zero , for, they are precisely $\overline{1}, \overline{2}, \cdots, \overline{p-1}$ in some order.

Similarly we can show that for any odd prime $p > 3$

$$1+\frac{1}{2^2}+\cdots+\frac{1}{(p-1)^2}\equiv 0 \pmod{p} \tag{2}$$

However, we are not aware of of any such algebraic interpretation of the next result which is known as Wolstenholme's theorem:

1.2.3 Theorem. *If p is a prime > 3, then*

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv 0 \pmod{p^2} \tag{3}$$

Proof. We have

$$\begin{aligned} & 1+\frac{1}{2}+\cdots+\frac{1}{p-1} \\ &= 1+\frac{1}{p-1}+\frac{1}{2}+\frac{1}{p-2}+\cdots+\frac{1}{\frac{p-1}{2}}+\frac{1}{\frac{p+1}{2}} \\ &= p\left(\frac{1}{p-1}+\frac{1}{2(p-2)}+\frac{1}{3(p-3)}+\cdots+\frac{1}{\frac{p-1}{2}\frac{p+1}{2}}\right) \end{aligned}$$

$$(4). \quad \equiv p\left(-1-\left(2^{-1}\right)^2-\left(3^{-1}\right)^2-\cdots-\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2\right) \pmod{p^2}$$

But,

$$1+\left(2^{-1}\right)^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2$$

$$\equiv \left(1^{-1}\right)^2+\left(2^{-1}\right)^2+\left(3^{-1}\right)^2+\cdots+\left((p-1)^{-1}\right)^2$$

$$-\left[\left(\left(\frac{p+1}{2}\right)^{-1}\right)^2+\cdots+\left((p-1)^{-1}\right)^2\right] \pmod{p}$$

$$\equiv -\left[\left(\left(p-\frac{p-1}{2}\right)^{-1}\right)^2+\cdots+\left((p-(p-1))^{-1}\right)^2\right] \pmod{p}$$

$$\equiv -\left[1+\left(2^{-1}\right)^2+\left(3^{-1}\right)^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2\right] \pmod{p}.$$

Hence,

$$2\left[1+\left(2^{-1}\right)^2+\left(3^{-1}\right)^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2\right] \equiv 0 \pmod{p}.$$

Therefore, from (4), we get

$$1+\frac{1}{2}+\cdots+\frac{1}{p-1} \equiv 0 \pmod{p^2}.$$

□

We give an alternative proof of (3), due to S.D. Chowla and A.Sreerama Sastri [1] which depends on the following basic result.

1.2.4 Lemma. *If* $1 \leq n < p-1$, *then*

$$S_n = 1 + 2^n + 3^n + \cdots + (p-1)^n \equiv 0 \pmod{p}.$$

Proof. We have

$$(x+1)^n - x^n = \binom{n}{1} x^{n-1} + \cdots + \binom{n}{n-1} + 1$$

Hence

$$p^n - 1 = \sum_1^{p-1} [(x+1)^n - x^n] = \binom{n}{1} S_{n-1} + \cdots + \binom{n}{n-1} S_1 + (p-1)$$

so that

$$\binom{n}{1} S_{n-1} + \cdots + \binom{n}{n-1} S_1 \equiv 0 \pmod{p}$$

Now, induction on n proves the lemma. □

Proof. Coming to the proof of the main theorem, note that Wolstenholme's congruence is equivalent to

$$\sum_{m<p/2} \left(\frac{1}{m} + \frac{1}{p-m}\right) \equiv 0 \pmod{p^2}$$

or

$$\sum_{m<p/2} \left(\frac{1}{m(p-m)}\right) \equiv 0 \pmod{p}$$

or

$$\sum_{m<p/2} \left(\frac{1}{m^2}\right) \equiv 0 \pmod{p}$$

which is equivalent to

(5). $$\sum_{m<p/2} \frac{m^{p-1}}{m^2} = \sum_{m<p/2} m^{p-3} \equiv 0 \pmod{p}$$

Since $p-3$ is even ,

$$m^{p-3} \equiv (p-m)^{p-3} \pmod{p}$$

,

and hence from (5)

$$\sum_{m<p} (m^{p-3}) \equiv 0 \pmod{p}$$

by lemma, since $p > 3$.

This completes the proof □

1.3 Generalisation of Fermat's Little Theorem

We begin by stating Eisenstein's generalisation of Fermat's Little Theorem:

1.3.1 Theorem. *For any prime $p > 3$, we have*

$$2^{p-1} \equiv 1 + p\left(1 + \frac{1}{3} + \cdots + \frac{1}{p-2}\right) \pmod{p^2}$$

Our proof is based on the following combinatorial identity ([17], pp. 27).

$$(6) \qquad \sum_{k=1}^{n} \frac{(1-x)^k}{k} = \sum_{k=1}^{n} \binom{n}{k} (-1)^k \frac{(x^k-1)}{k} \quad \forall n \in N,\ x \in R,$$

For a different proof, see Hardy and Wright [10].

Proof. Putting $n = p$, and $x = 2$ in the identity,we obtain

$$\sum_{k=1}^{p} \frac{(1-2)^k}{k} = \sum_{k=1}^{p} \binom{p}{k} (-1)^k \frac{(2^k-1)}{k}$$

$$= p \sum_{k=1}^{p-1} \binom{p-1}{k-1} (-1)^k \frac{(2^k-1)}{k} - \frac{(2^p-1)}{p}$$

since

$$\binom{p}{k} = \frac{p}{k} \binom{p-1}{k-1}$$

Therefore,

$$(7) \qquad \sum_{k=1}^{p} \frac{(-1)^k}{k} \equiv -\frac{2^p-1}{p} \pmod{p}$$

But

$$1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{p-1} \equiv 2\left(1 + \frac{1}{3} + \cdots + \frac{1}{p-2}\right) \pmod{p}$$

Hence from (6),

$$-2\left(1 + \frac{1}{3} + \cdots + \frac{1}{p-2}\right) - \frac{1}{p} \equiv -\frac{2^p-1}{p} \pmod{p}$$

or

$$2^{p-1} \equiv 1 + p\left(1 + \frac{1}{3} + \cdots + \frac{1}{p-2}\right) \pmod{p^2}.$$

□

The simplicity of Eisenstein's congruence will be perhaps lost when we try to extend it to the case of p^3, as is evident in the following result of P. Jothilingam [12].

1.3.2 Theorem. *For an odd prime $p > 3$,*

$$2^{p-1} \equiv 1 + p\left(1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{(p-2)}\right) - p^2 \sum_{s=1}^{a} \left(b_s + (\frac{2}{p}) b_{a-s+1}\right) 2^{s-1} \pmod{p^3}.$$

where $(\frac{2}{p})$ is a Legendre symbol and $b_1, b_2, \cdots b_a$ are quadratic residues modulo p.

Proof. Putting $x = 2$ and $n = p > 3$, an odd prime in the identity (6)

$$\sum_{k=1}^{p} \frac{(-1)^k}{k} = \sum_{k=1}^{p} \binom{p}{k} \frac{(-1)^k}{k} (2^k - 1)$$

$$= p \sum_{k=1}^{p-1} \binom{p-1}{k-1} \frac{(-1)^k}{k^2} (2^k - 1) - \frac{(2^p - 1)}{p}$$

since

$$\binom{p}{k} = \frac{p}{k} \binom{p-1}{k-1}.$$

Therefore,

$$\sum_{k=1}^{p} \frac{(-1)^k}{k} \equiv -p \sum_{k=1}^{p-1} \frac{2^k - 1}{k^2} - \frac{(2^p - 1)}{p} \pmod{p^2}$$

$$\equiv -p\sum_{k=1}^{p-1}\frac{2^k}{k^2}-\frac{(2^p-1)}{p} \pmod{p^2} \tag{8}$$

as

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(p-1)^2}\equiv 0 \pmod{p}$$

But

$$1-\frac{1}{2}+\frac{1}{3}-\cdots-\frac{1}{p-1}\equiv 2\left(1+\frac{1}{3}+\cdots+\frac{1}{p-2}\right) \pmod{p^2},$$

by Wolstenholme's congruence. Therefore, from (8),

$$2\left(1+\frac{1}{3}+\cdots+\frac{1}{p-2})+\frac{1}{p}\right)\equiv p\sum_{k=1}^{p-1}\frac{2^k}{k^2}+\frac{2^p-1}{p} \pmod{p^2}.$$

or

$$2^{p-1}\equiv 1+p\left(1+\frac{1}{3}+\cdots+\frac{1}{p-2}\right)-p^2\sum_{k=1}^{p-1}\frac{2^{k-1}}{k^2} \pmod{p^3} \tag{9}$$

By Euler's criterion,

$$2^{(p-1)/2}\equiv\left(\frac{2}{p}\right) \pmod{p}.$$

Hence,

$$2^{a+k}\equiv 2^k\left(\frac{2}{p}\right) \pmod{p}.$$

So

$$\sum_{k=1}^{p-1} \frac{2^{(k-1)}}{k^2} = \sum_{k=1}^{a} \frac{2^{(k-1)}}{k^2} + \sum_{k=1}^{a} \frac{2^{a+k-1}}{(a+k)^2} \equiv \sum_{k=1}^{a} \frac{2^{k-1}}{k^2} + \sum_{k=1}^{a} \frac{2^{k-1}}{(a+k)^2} \left(\frac{2}{p}\right)$$

$$\equiv \sum_{k=1}^{a} \left(\frac{1}{k^2} + \left(\frac{2}{p}\right) \frac{1}{(a+k)^2}\right) 2^{k-1}$$

$$\equiv \sum_{1}^{a} \left(\frac{1}{k^2} + \left(\frac{2}{p}\right) \frac{1}{(a-k+1)^2}\right) 2^{k-1} \pmod{p}$$

since $a + k \equiv -(a - k + 1) \pmod{p}$. Let $b_1, b_2, \cdots, b_a$ be the residues of $1/1^2, 1/2^2, \cdots, 1/a^2 \bmod p$. Then these are also the quadratic residues modulo p. Using this in (9) we get

$$2^{p-1} \equiv 1 + p\left(1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2}\right) - p^2 \sum_{k=1}^{a} \left(b_k + \left(\frac{2}{p}\right) b_{a-k+1}\right) 2^{k-1} \pmod{p^3}$$

□

Our attempt to obtain a congruence for $3^{p-1} \bmod p^2$ similar to Eisenstein's congruence in its simplicity, in the same manner, has not been successful. The difficulty lies in finding a closed form for the residue of

$$\sum_{k=1}^{p-1} \frac{(-2)^k}{k} \pmod{p}.$$

However, in the next section we find a nice formula for $3^{p-1} \bmod p^2$ using what is known as "Fermat quotient".

1.4 Fermat quotient

For any prime p and any integer a, p not dividing a, we let the Fermat quotient $F(a)$ to be

$$F(a) = \frac{a^{p-1} - 1}{p}.$$

In terms of $F(a)$, Eisenstein's congruence can be written as

$$F(2) \equiv 1 + \tfrac{1}{3} + \cdots + \tfrac{1}{p-2} \pmod{p}.$$

Thus a complete generalisation of Fermat's Little Theorem similar to Eisenstein's result requires us to find a easily calculable residue of $F(a)$ mod p. We begin with a brief disscussion on the basic properties of $F(a)$. We have

$$F(ab) \equiv F(a) + F(b) \pmod{p},$$

since

$$\begin{aligned}(ab)^{p-1} &= (1 + pF(a))(1 + pF(b)) \\ &\equiv 1 + p(F(a) + F(b)) \pmod{p^2}.\end{aligned}$$

Thus $F(a)$ modulo p behaves like a logarithm. We also have

$$F(a + pt) \equiv f(a) - \bar{a}t \pmod{p},$$

where $a\bar{a} \equiv 1 \pmod{p^2}$.

In fact,

$$\begin{aligned}(a + pt)^{p-1} &\equiv a^{p-1} + p(p-1)ta^{p-2} \pmod{p^2}) \\ &\equiv 1 + pF(a) + p(p-1)ta^{p-1}\bar{a} \pmod{p^2} \\ &\equiv 1 + pF(a) + p(p-1)t\bar{a}(1 + pF(a)) \pmod{p^2} \\ &\equiv 1 + p(F(a) + (p-1)t\bar{a}) \pmod{p^2}\end{aligned} \tag{10}$$

Using the above properties of $F(a) \bmod p$, we now derive a general formula for $F(a)$ modulo p, following Ram Murty [15]. By the logarithmic property of F, we have

$$\sum_{j=1}^{p-1} F(aj) \equiv \sum_{j=1}^{p-1} F(a) + \sum_{j=1}^{p-1} F(j) \pmod{p}$$

,

which yields the following relation easily.

$$F(a) \equiv \sum_{j=1}^{p-1} F(j) - \sum_{j=1}^{p-1} F(aj) \pmod{p}$$

.

Let $aj = pq_j + r_j$, with $1 \leq r_j \leq p-1$. Then

$$F(aj) = F(r_j + pq_j) \equiv F(r_j) - r_j q_j \pmod{p},$$

by (10). As j runs through 1 to $p-1$ so does r_j. Therefore,

(11). $$F(a) \equiv \sum_{j=1}^{p-1} \frac{q_j}{r_j} \equiv \sum_{j=1}^{p-1} \left[\frac{ja}{p}\right] \frac{1}{ja} \pmod{p}$$

which is the formula for $F(a)$ as alluded to earlier. We first show that this formula can be used to give another derivation of Eisenstein's Congruence. We begin with the formula for $a = 2$, namely,

$$F(2) \equiv \frac{1}{2} \sum_{j=1}^{p-1} \left[\frac{2j}{p}\right] \frac{1}{j} \pmod{p}$$

.

But

$$\left[\frac{2j}{p}\right] = 0, \Leftrightarrow 1 \leq j \leq (p-1)/2$$

since $2j/p < 1 \Leftrightarrow j < p/2 = (p-1)/2 + 1/2$, i.e. $j \leq (p-1)/2$.

Similarly,

$$\left[\frac{2j}{p}\right] = 1 \quad \Leftrightarrow \quad (p+1)/2 \leq j \leq p-1.$$

Therefore,

$$\frac{2^p - 2}{p} \equiv \sum_{j=(p+1)/2}^{p-1} \frac{1}{j} \pmod{p}$$

$$\equiv -\sum_{j=1}^{(p-1)/2} \frac{1}{j} \pmod{p}.$$

This can also be written as

$$\frac{2^{p-1} - 1}{p} \equiv -\frac{1}{2} \sum_{j=1}^{(p-1)/2} \frac{1}{j}.$$

On the other hand,

$$-\frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{(p-1)/2}\right) \equiv \sum_{j=1}^{p-1} \frac{1}{j} - \frac{1}{2} \sum_{j=1}^{(p-1)/2} \pmod{p}$$

$$\equiv \sum_{j=1}^{p-1} \frac{1}{j} - \left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{p-1}\right) \pmod{p}$$

$$\equiv 1 + \frac{1}{3} + \cdots + \frac{1}{p-2} \pmod{p}.$$

so that

$$\frac{2^{p-1} - 1}{p} \equiv 1 + \frac{1}{3} + \cdots + \frac{1}{p-2} \pmod{p}.$$

which is Eisenstein's congruence (Theorem 1.0.5).

We now derive a formula for $3^{p-1} \bmod p^2$ which generalises Eisenstein's congruence. We first compute $F(3)$ with respect to a prime p such that $(3,p) = 1$.

Now

$$\frac{3^p - 3}{p} \equiv \sum_{j=1}^{p-1} [3j/p] \frac{1}{j} \pmod{p} \tag{12}$$

so that our task reduces to working out$[3j/p]$. Consider the case when $3|p-1$

.

We have

$3j/p < 1 \Leftrightarrow j < p/3 = (p-1)/3 + 1/3$, i.e., $j \leq (p-1)/3$,

which implies that these $j's$ do not contribute to the sum in (12). Similarly we can show that for

$$\frac{p+2}{3} \leq j \leq \frac{2(p-1)}{3}$$

the corresponding terms in the sum will contribute 1 and for

$$\frac{2p+1}{3} \leq j \leq p-1,$$

they will contribute 2 . Hence (12) can be simplified to

$$3F(3) \equiv 0 + \sum_{j=(p+2)/3}^{2(p-1)/3} \frac{1}{j} + \sum_{j=(2p+1)/3}^{p-1} \frac{2}{j} \pmod{p}$$

$$\equiv \sum_{j=1}^{(p-1)/3} \frac{1}{j} + \sum_{j=(p+2)/3}^{2(p-1)/3} \frac{1}{j} + \sum_{j=(2p+1)/3}^{p-1} \frac{1}{j} + \sum_{j=(2p+1)/3}^{p-1} \frac{1}{j} - \sum_{j=1}^{(p-1)/3} \frac{1}{j} \pmod{p}$$

EASTERN HILL UNIVERSITY LIBRARY 103327 28-3-05

$$\equiv \sum_{j=1}^{p-1} \frac{1}{j} + \sum_{j=(2p+1)/3}^{p-1} \frac{1}{j} - \sum_{j=1}^{(p-1)/3} \pmod{p}$$

Note that the first term is congruent to 0 mod p by (1). Changing j to $p-j$ makes it clear that the second term is congruent to

$$-\sum_{j=1}^{(p-1)/3} \frac{1}{j} \bmod p.$$

Thus, in case $3|p-1$, we see that

$$3F(3) \equiv -2 \sum_{j=1}^{(p-1)/3} \frac{1}{j} \pmod{p}$$

.

In case $3|p+1$ or equivalently $3|p-2$, an equally pleasant calculation shows that the terms in the sum in (12) contribute 0 for $j \leq (p-2)/3$, contribute 1 each for $(p+1)/3 \leq j \leq (2p-1)/3$ and contribute 2 each for $2(p+1)/3 \leq j \leq p-1$. Thus from (12) we get

$$3F(3) \equiv 0 + \sum_{j=(p+1)/3}^{(2p-1)/3} \frac{1}{j} \sum_{j=2(p+1)/3}^{p-1} \frac{2}{j} \pmod{p}$$

$$\equiv \sum_{j=1}^{(p-2)/3} \frac{1}{j} + \sum_{j=(p+1)/3}^{(2p-1)/3} \frac{1}{j} + \sum_{j=2(p+1)/3}^{p-1} \frac{1}{j} + \sum_{j=2(p+1)/3}^{p-1} \frac{1}{j} - \sum_{j=1}^{(p-2)/3} \frac{1}{j} \pmod{p}$$

$$\equiv \sum_{j=1}^{p-1} \frac{1}{j} - \sum_{j=1}^{(p-2)/3} \frac{1}{j} - \sum_{j=1}^{(p-2)/3} \frac{1}{j} \pmod{p}$$

$$\equiv -2 \sum_{j=1}^{(p-2)/3} \frac{1}{j} \pmod{p}.$$

So we have proved

1.4.1 Theorem. *For any prime $p > 3$,*

$$3^{p-1} \equiv 1 - \frac{2}{3} p \sum_{j=1}^{(p-2)/3} \frac{1}{j} \pmod{p^2},$$

if $3|p+1$ *and*

$$3^{p-1} \equiv 1 - \frac{2}{3} p \sum_{j=1}^{(p-1)/3} \frac{1}{j} \pmod{p^2},$$

if $3|p-1$.

1.5 Wieferich Primes

A prime p satisfying $2^{p-1} \equiv 1 \pmod{p^2}$ is called a Wieferich prime.

The primes 1093 and 3511 were proved to be Wieferich primes by Meissner and Beeger in 1913 and 1922 (Ribenboim [16]) respectively. Recently it has been announced after a computer search that there are no other Wieferich primes below 10^{15}. However, we can still ask

(1) Are there infinitely many primes p such that

$$2^{p-1} \equiv 1 \pmod{p^2}$$

or

(2)Are there infinitely many primes p which do not satisfy Wieferich's congruence?

While it seems that very few primes satisfy Wieferich's congruence, M.Ram Murty's work [15] has indicated that there are infinitely many such primes which are not Wieferich primes. We follow his treatment below.

A positive integer is squarefree if it not divisible by a square, otherwise, it is said to be squarefull.

Let

$$2^n - 1 = u_n v_n$$

where u_n is squarefree and v_n is squarefull, $(u_n, v_n) = 1$. Suppose $p|u_n$, i.e. $p|2^n - 1$ but $2^n \not\equiv 1 \pmod{p^2}$. Let $d = o(2) \bmod p$. Then $p - 1 = dx$ and $n = dy$ for some integers x and y. Let $2^d = 1 + pm$. Then

$$2^n = (1 + pm)^y \equiv 1 + pmy \pmod{p^2}$$

where $(my, p) = 1$ and

$$2^{p-1} = (1 + pm)^x \equiv 1 + pmx \pmod{p^2}$$

where $(mx, p) = 1$ i.e. $2^{p-1} \not\equiv 1 \pmod{p^2}$.

By the ABC conjecture,

$$u_n\, v_n \leq (u_n v_n^{1/2})^{1+\epsilon}$$

so that $v_n \leq 2^{n\epsilon}$ which means that $u_n \to \infty$.

The sequence u_q is mutually coprime for primes q, since if d is the order of 2 mod p where p is a prime factor of both u_m and u_n and m, n are distinct primes, then $p|m$ and $p|n$ which is not possible.Hence there are infinitely many primes p such that

$$2^{p-1} \not\equiv 1 \pmod{p^2},$$

settling question (2).

Question (1) as we have indicated is no closer to settlement. However we may note that an odd prime p is a Wieferich prime

(1) if and only if

$$1+\frac{1}{3}+\cdots+\frac{1}{p-2} \equiv 0 \pmod{p}$$

by Eisenstein's Congruence, or

(2) if and only if

$$1+\frac{1}{2}+\cdots+\frac{1}{\frac{p-1}{2}} \equiv 0 \pmod{p}$$

by our formula for $F(2)$.

1.6 Generalisation of Wolstenholme's thoerem

We discuss a couple of interesting congruences which generalise Wolstenholme's congruence. The first is due to Chowla [2].

1.6.1 Theorem. *If a prime $p > 3$ then*

$$\sum_{n<p^{2m}} \frac{1}{n} \equiv 0 \pmod{p^{2m}} \tag{13}$$

where $(n,p) = 1$.

Proof. Congruence (13) is same as

$$\sum_{n<\frac{1}{2}p^m} (\frac{1}{n}+\frac{1}{p^m-n}) \equiv 0 \pmod{p^{2m}}$$

where $(n,p)=1$.

i.e.
$$\sum_{n<\frac{1}{2}p^m} \frac{1}{n(p^m-n)} \equiv 0 \pmod{p^m}$$

or

(14)
$$\sum_{n<\frac{1}{2}p^m} \frac{1}{n^2} \equiv 0 \pmod{p^m}$$

By Fermat's little theorem,
$$n^{(p-1)p^{(m-1)}} \equiv 1 \pmod{p^m}$$

so that (14) reduces to

(15)
$$\sum_{n<\frac{1}{2}p^m} \frac{n^{p^{(m-1)}(p-1)}}{n^2} = \sum_{n<\frac{1}{2}p^m} n^{p^{m-1}(p-1)-2} \equiv 0 \pmod{p^m}$$

Since $p^{m-1}(p-1)-2$ is even,
$$n^{p^{m-1}(p-1)-2} \equiv (p^m-n)^{p^{m-1}(p-1)-2} \pmod{p^m}$$

so that (15) is equivalent to

(16)
$$\sum_{n<p^m} n^{p^{m-1}(p-1)-2} \equiv 0 \pmod{p^m}$$

To prove (16), let g be a primitive root of p^m and let

$$s = \phi(p^m) = p^{m-1}(p-1), \quad t = s - 2.$$

Then (16) is equivalent to

$$\sum_{n=1}^{s} g^{tn} \equiv 0 \pmod{p^m}$$

or to

$$\frac{g^t(g^{ts}-1)}{g^t - 1} \equiv 0 \pmod{p^m}.$$

This is true because $g^s \equiv 1 \pmod{p^m}$ and g^t is not congruent to 1 mod p. Hence the proof. □

The following result is known as Leudesdorf's generalisation of Wolstenholme's theorem (Chowla [2]).

1.6.2 Theorem. *If* $(n, 6) = 1$, *then*

$$\sum_{m<n}{}' \left(\frac{1}{m}\right) \equiv 0 \pmod{n^2}$$

where the dash means $(n, m) = 1$

Proof.

$$\sum_{m<n}{}' \left(\frac{1}{m}\right) \equiv 0 \pmod{n^2} \Leftrightarrow \sum_{m<n}{}' \left(\frac{1}{m(n-m)}\right) \equiv 0 \pmod{n}$$

$$\Leftrightarrow \sum_{m<n}{}' (\frac{1}{m^2}) \equiv 0 \pmod{n}$$

If $(a,n) = 1$ and a^2 is not congruent to 1 mod n then

$$\sum{}' m^{-2} \equiv \sum{}' (am)^{-2} \pmod{n}$$

or

$$(a^{-2} - 1) \sum{}' m^{-2} \equiv 0 \pmod{n}$$

Hence the proof □

1.7 Some Assorted Congruences

The following congruence is due to Winfried Kohnen [14]. Our interest in this congruence is because the proof uses the same combinatorial identity which we had utilised to derive Eisenstein's Congruence.

1.7.1 Theorem. *Let p be an odd prime. Then*

$$\sum_{k=1}^{p-1} \frac{1}{k\,2^k} \equiv \sum_{k=1}^{(p-1)/2} \frac{(-1)^{k-1}}{k} \pmod{p}.$$

Proof. Putting $x = 1$ and $n = p - 1$ in the identity (6) and observing that

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

and

$$\sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p}.$$

we obtain

$$\sum_{k=1}^{p-1} \frac{2^k}{k} \equiv \sum_{k=1}^{p-1} \frac{(-1)^k}{k} \pmod{p} \tag{17}$$

In the sum on the left, replace k by $p-k \equiv -k \pmod{p}$ and use Fermat's Little Theorem to get

$$\sum_{k=1}^{p-1} \frac{2^k}{k} \equiv -2^p \sum_{k=1}^{p-1} \frac{1}{k\,2^k} \equiv -2 \sum_{k=1}^{p-1} \frac{1}{k\,2^k} \pmod{p}.$$

The sum on the right of (17) can be written as

$$\sum_{k=1}^{(p-1)/2} \frac{(-1)^k}{k} + \sum_{k=1}^{(p-1)/2} \frac{(-1)^{p-k}}{p-k} \equiv 2 \sum_{k=1}^{(p-1)/2} \frac{(-1)^k}{k} \pmod{p}.$$

This proves the theorem. □

A slightly more complicated congruence, as stated in the next theorem due to Zhi-Wei Sun [19], however needs vastly deeper techniques. In fact, Sun's proof is quite unusual as it uses properties of some Pell sequence.

1.7.2 Theorem. *For an odd prime p*

$$\sum_{k=1}^{(p-1)/2} \frac{1}{k\,2^k} \equiv \sum_{k=1}^{[3p/4]} \frac{(-1)^{k-1}}{k} \pmod{p}$$

We omit the proof as it is long and complicated. Since the summands of the righthand side of the above congruence is related to the combinatorial identity we have repeatedly used, it may be possible to give a shorter and elegant proof using that identity.

To complete the chapter we present yet another congruence of binomial coefficients due to Chowla .

1.7.3 Theorem. *For all primes $p \geq 5$,*

$$\binom{2p}{p} \equiv 2 \pmod{p^3}.$$

Proof.

$$\binom{2p}{p} = \frac{2p(p+p-1)(p+p-2)\cdots(p+2)(p+1)}{1\cdot 2\cdot 3\cdots(p-1)p}$$

$$= \frac{2\prod_{x=1}^{p-1}(p+x)}{(p-1)!} = \frac{2\prod_{x=1}^{p-1}(1+p/x)\prod_{x=1}^{p-1}x}{\prod_{x=1}^{p-1}x}$$

$$= 2\prod_{x=1}^{p-1}(1+p/x)$$

$$\equiv 2 + 2p\sum_{x=1}^{p-1}\frac{1}{x} + 2p^2\sum\frac{1}{xy} \pmod{p^3} \tag{18}$$

where $1 \leq x < y \leq p-1$.

But,

$$2\sum\frac{1}{xy} = (\sum_{x=1}^{p-1}(\frac{1}{x}))^2 - \sum_{x=1}^{p-1}(\frac{1}{x^2}).$$

And as we have seen before,

$$\sum_{x=1}^{p-1}\frac{1}{x} \equiv 0 \pmod{p^2}$$

and
$$\sum_{x=1}^{p-1} \frac{1}{x^2} \equiv 0 \pmod{p}.$$

Therefore, the last two terms of (18) are congruent to 0 mod p^3. Hence the theorem. □

Chapter 2

Congruences Involving Bernoulli Numbers

2.1 Introduction

The choice of the subject of this chapter may seem surprising. However, the object is to understand Voronoi's Congruence [11], as Voronoi type sums occur in calculations involving Fermat quotients. Also we present Chowla's clever use of Von Staudt's theorem in establishing Wolstenholme's congruence so as to give a proof of different flavour.

2.2 Basic properties of Bernoulli Numbers

Bernoulli numbers B_n (n non-negative) are defined by the relation

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n t^n}{n!}$$

The following are the properties which can be quickly established:

(1) Bernoulli numbers satisfy the recurrence relation

$$\sum_{i=1}^{m} \binom{m}{i} B_{m-i} = 0$$

so that

$$B_0 = 1, \ B_1 = -1/2, \ B_2 = 1/6, \ B_4 = -1/30, \ B_6 = 1/42, \ B_8 = -1/30, \ \cdots$$

(2) As

$$\frac{t}{e^t - 1} + \frac{t}{2}$$

is an even function of t,

$$B_{2m+1} = 0$$

for all $m \geq 1$.

(3) If

$$S_m(n) = 1^m + 2^m + \cdots + (n-1)^m$$

where $m \geq 1$, then

$$(m+1)S_m(n) = \sum_{k=0}^{m} \binom{m+1}{k} n^{m+1-k} B_k$$

which can further be simplified to

$$S_m(n) = \sum_{i=0}^{m} \binom{m}{i} B_{m-i} \frac{n^{i+1}}{i+1} \tag{1}$$

The details may be found in [11]

2.3 Congruences

We now begin the preparation for deriving Voronoi's congruence. Our treatment closely follows that of Ram Murty[15].

A rational number $x/y \neq 0$ is p-integral (p is a prime) if p does not divide the denominator y. The order of the rational number x/y denoted $ord_p(x/y)$ is defined as $ord_p x - ord_p(y)$ where $ord_p(a)$ for an integer a is the highest power of p dividing a. We begin with the simple observation

2.3.1 Lemma. *For an odd prime p, pB_k is p-integral.*

Proof. The proof is by induction on m. Setting $n = p$ in (1) we have

$$S_m(p) = pB_m + \sum_{i=1}^{m} \binom{m}{i} pB_{m-i} \frac{p^{i+1}}{i+1}.$$

Since $p^i \geq 2^i \geq i+1$, it follows that $ord_p(p^i/i+1) \geq 0$ and by induction hypothesis each pB_{m-i} in the sum is p-integral. But $S_m(n)$ is an integer. Therefore pB_m is p-integral. □

It follows from this lemma that, if $B_k = U_k/V_k$ with $(U_k, V_k) = 1$, then V_k is not divisible by p^2 and that

$$S_m(n) \equiv pB_m \pmod{p}.$$

We also have

2.3.2 Lemma. *If $p-1$ does not divide k, then $S_k(p) \equiv 0 \pmod{p}$ and if $p-1|k$, then $S_k(p) \equiv -1 \pmod{p}$.*

Proof. Let g be a primitive root mod p. Then, if $p-1$ does not divide k,

$$S_k(p) \equiv \sum_{j=0}^{p-2} (g^j)^k \equiv \frac{g^{k(p-1)} - 1}{g^k - 1} \equiv 0 \pmod{p}.$$

If $p-1|k$, then by Fermat's Little Theorem

$$S_k(p) \equiv p - 1 \equiv -1 \pmod{p}.$$

Now we can prove

2.3.3 Theorem. *(Von Staudt-Clausen) For an even integer k,*

$$B_k + \sum_{p-1|k} \frac{1}{p}$$

is an integer.

Proof. From the last two lemmas, we observe that if $p-1$ does not divide k, then

$$pB_k \equiv 0 \pmod{p}$$

and so $B_k + 1/p$ cannot be p-integral and if $p-1|k$ then

$$pB_k \equiv -1 \pmod{p}$$

i.e., $pB_k + 1 \equiv 0 \pmod{p}$.

In this case, V_k is square-free which means that the prime factors of V_k are precisely those p's such that $p-1|k$. Since $pB_k + 1 \equiv 0 \pmod{p}$ means that

$$B_k + \frac{1}{p}$$

is p-integral for each such prime p,it follows that

$$B_k + \sum_{p-1|k} \frac{1}{p}$$

is an integer.

We can now derive Voronoi congruences. These are

2.3.4 Theorem. *For an even integer $k \geq 2$, we have*

$$V_k \, S_k(n) \equiv U_k \, n \pmod{n^2}$$

2.3.5 Theorem. *For a positive integer n with $(n,a) = 1$, we have*

$$(a^k - 1)S_k(n) \equiv kna^{k-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] j^{k-1} \pmod{n^2}.$$

Proof. For each j with $1 \leq j < n$, we can write $ja = q_j n + r_j$ where $0 \leq r_j < n$ so that

$$q_j = \left[\frac{ja}{n}\right].$$

Thus we have

$$\begin{aligned}(ja)^k &\equiv r_j^k + kq_j n r_j^{k-1} \pmod{n^2} \\ &\equiv r_j^k + kq_j n(ja)^{k-1} \pmod{n^2}\end{aligned}$$

As j varies from 1 to $n-1$, so does r_j since $(a,n)=1$. Summing the above congruence over j from 1 to $n-1$ we get the required congruence. □

We complete the chapter by disscussing an ingenious proof of the generalisation congruence of Wolstenholme's congruence due to Chowla which uses Von Staudt's theorem.

2.3.6 Theorem.

$$\sum_{n \leq p^{2m}}{}' \frac{1}{n} \equiv 0 \pmod{p^{2m}}$$

Where the dash indicates that n is prime to p

Proof. If n is prime to p then

$$n^{p^{2m}-p^{2m-1}} \equiv 1 \pmod{p^{2m}}$$

$$\Rightarrow \sum_{n \leq p^{2m}}{}' \frac{1}{n} \equiv \sum_{n \leq p^{2m}}{}' n^{p^{2m}-p^{2m-1}-1} \pmod{p^{2m}} \tag{2}$$

Now

$$p^{2m} - p^{2m-1} - 1 > 2m$$

since $p \geq 3$

Hence (2) becomes

$$\sum_{n \leq p^{2m}}{}' \frac{1}{n} \equiv \sum_{n \leq p^{2m}} n^{p^{2m} - p^{2m-1} - 1} \pmod{p^{2m}} \tag{3}$$

where the dash is removed from the right hand side.

Now

$$\sum_{s \leq p^{2m}} s^a = \frac{p^{m(a+1)}}{a+1} + \frac{1}{2}p^{ma} + \binom{a}{1}\frac{B_1}{2}p^{m(a-1)}$$

$$-\binom{a}{3}\frac{B_2}{4}p^{m(a-3)} + \cdots + \pm\binom{a}{a-2}\frac{B_{(a-1)/2}}{a-1}p^{2m} \tag{4}$$

where

$$a = p^{2m} - p^{2m-1} - 1,$$

and $B_1, B_2, \ldots$ are Bernoulli's numbers.

We now apply Von Staudt's theorem on Bernoulli's numbers in equation (4). Von Staudt's theorem says that the denominator of B_n in its lowest terms is a *quadratfrei* number, all of whose prime factors q satisfy $2n \equiv 0 \pmod{q-1}$. Now the last term in (4) is

$$\pm\frac{1}{2}aB_{\frac{1}{2}(a-1)}p^{2m} \tag{5}$$

If the denominator of

$$B_{\frac{1}{2}(a-1)}$$

is divisible by p, then, by Vonstaudt's theorem,

$$a-1=p^{2m}-p^{2m-1}-2$$

is divisible by $p-1$. This is not possible if $p>3$. If $p=3, p$ may occur as a factor only once. It follows that the numerator of $\pm\frac{1}{2}aB_{\frac{1}{2}(a-1)}p^{2m}$ is divisible by p^{2m} when $p>3$, and by 3^{2m-1} when $p=3$.
Then by Von Staudt's theorem the terms in (4) that occur before

$$\pm\frac{1}{2}aB_{\frac{1}{2}(a-1)}p^{2m}$$

exept the first are divisible by p^{2m} if

$$mp^{2m-1}(p-1)\geq 4m-1,$$

which is true if $p\geq 3$. Hence

(6) $$\sum_{s\leq 3^{2m}} s^a\equiv 0 \pmod{p^{2m}}$$

if $p>3$, and

(7) $$\sum_{s\leq 3^{2m}} s^a\equiv 0 \pmod{3^{2m-1}}$$

Finally, from (3) and (6) we get the required result. This also proves

$$\sum_{n\leq 3^{2m}}{}' \frac{1}{n} \equiv 0 \pmod{3^{2m-1}}.$$

Chapter 3

p-adic Numbers And p-adic Analysis

3.1 Introduction

This chapter is a brief review of p-adic fields. We gather here the concepts and results (without any proof) from "p-adic analysis" which we shall require in the next chapter. Our basic references for the material are Koblitz [13] and Robert [18]. Washington [20] is quite helpful for p-adic gamma function and related matters.

3.2 p-adic fields

Let p be a prime. Recall that for any nonzero integer a, $ord_p(a)$ is the highest power of p dividing a. The concept was extended to rationals by setting $ord_p(r) = ord_p(a) - ord_p(b)$ if $r = a/b$. We use this idea to define a norm on Q. More specifically, if $|\ |_p$ on Q is defined by

$$|x|_p = \begin{cases} \frac{1}{p^{ord_p(x)}} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

then $|\ |_p$ is a norm on Q. In fact, it satisfies a stronger non-Archimedean property, namely

$$|x + y|_p \leq max\{|x|_p + |y|_p\}.$$

The corresponding metric on Q, defined by

$$d(x, y) = |x - y|_p$$

is also non-Archimedean in the sense that

$$d(x, y) \leq max\ \{d(x, z)\ , d(z, y)\}$$

for any x, y, z in Q.

Thus for every prime p, we have a non-Archimedean metric on Q, in contrast to the usual metric on Q induced by the absolute value which is an Archimedean one, i.e., not non-Archimedean.

The famous theorem of Ostrowski says that every non-trivial norm on Q is essentially either $|\ |_p$ for some prime p or the usual absolute value. Note

that for any prime p, the nonzero values of the p-adic norm on Q are integral powers of p.

By a well-known construction using cauchy sequences, any metric space can be completed. When completed in this manner, for example, Q with the usual metric yields the complete field of real numbers. In a similar manner, for any fixed prime p, we can complete Q with respect to the p-adic metric to obtain the the field of p-adic numbers Q_p. Thus elements of Q_p are equivalence classes of cauchy sequences of rational numbers. The p-adic norm of Q can be extended to Q_p as follows : For any a in Q_p, if $\{a_n\}$ is a cauchy sequence which represents the class of a, let

$$|a|_p = lim_{n\to\infty}|a_n|_p$$

It can be easily verified that this is well-defined and that it is a norm. It is a routine matter to verify that Q_p is complete with respect to this norm. Observe that, unlike the real case, the nonzero value of the extended norm is the same as that of the norm on Q, namely the integral powers of p.

There is a more practical description of elements of Q_p other than being equivalence classes of cauchy sequences. This new description depends on the following fact (Koblitz [13]): For any a in Q_p with $|a|_p \leq 1$, there is a unique representative cauchy sequence $\{a_i\}$ of rational integers such that

(1) $$0 \leq a_i < p^i, \quad i = 1, 2, 3, \cdots$$

(2) $$a_i \equiv a_{i+1} \pmod{p^i} \quad i = 1, 2, 3, \cdots$$

Now let, for each i,

$$a_i = b_0 + b_1 p + \cdots + b_{i-1} p^{i-1}$$

be the ordinary expansion in base p, where $0 \leq b_j \leq p-1$. The condition (2) then shows that

$$a_{i+1} = b_0 = b_1 p + \cdots + b_{i-1} p^{i-1} + b_i p^i$$

for some b_i, $0 \leq b_i \leq p-1$.Thus the original a can be thought of as a "number" written in base p, which extends indefinitely to the right. In general, for any a in Q_p, choose the correct power of p such that $|p^m a|_p \leq 1$, whence it follows that $a \in Q_p$, in general has a Laurent series expansion:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + \cdots$$

This is the p-adic expansion of a.

Those numbers whose p-adic expansion has no negative powers of p, do form a subring of Q_p; this is the ring of p-adic integers, and is denoted by Z_p. Thus, $Z_p = \{a \in Q_p : |a|_p \leq 1\}$. Since any element of Z_p can be approximated by rational integers to any degree needed, Z is dense in Z_p. We also note that Z_p is compact.

3.3 p-adic series, Hensel's lemma

That analysis is easier in Q_p than in the complex field is due to the following fact:

3.3.1 Theorem. *A series* $\sum a_n$ $(a_n \in Q_p)$ *converges iff* $|a_n|_p \to 0$ *as* $n \to \infty$.

This theorem is a direct consequence of the non-archimedean nature of the p-adic metric.

for example, the series

$$\sum_{n=0}^{\infty} p^n$$

converges in Q_p to $1/(p-1)$.

We may consider power series over Q_p also. As in complex analysis, the power series

$$\sum_{n=0}^{\infty} a_n \, x^n \quad (a_n \in Q_p)$$

has radius of convergence r given by

$$r = \frac{1}{lim\ sup |a_n|_p^{1/n}}$$

where the usual conventions apply for $r = 0$ and $r = \infty$.

The exponential series

$$Exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

has radius of convergence

$$r = p^{-1/(p-1)},$$

whereas the "p-logarithm" series

$$\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

has radius of convergence $r = 1$. Thus the p-adic logarithm $\log_p(x)$ is defined by the power series for $|x-1|_p < 1$. It is easily checked that

$$\log_p(xy) = \log_p(x) + \log_p(y)$$

as an identity of formal power series.

To illustrate the power of these concepts in settling questions of congruences, we present the following example due to Ram Murty : Consider the series

$$\sum_{n=1}^{\infty} \frac{2^n}{n}$$

which converges in the 2-adic field Q_2 to $-\log(-1)$ by the definition of power series for logarithm. But observe that $-2\log(-1) = -\log 1 = -\log 1 = 0$. In other words, the given series converges to zero in Q_2. This can be interpreted as : For each positive integer m, there is a natural number n s.t.

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots + \frac{2^n}{n} \equiv 0 \pmod{2^m}.$$

An important tool for analysing functions over Q_p is the following:

3.3.2 Theorem. *Hensel's lemma: Let $f(x) \in Z_p[x]$ be a polynomial with coefficients in Z_p. If $f(x) \equiv 0 \pmod{p}$ has a solution $a_0 \in Z_p$ such that*

$f'(a_0) \not\equiv 0 \pmod{p}$, *then there is a unique* $a \in Z_p$ *s.t.* $f(a) = 0$ *where* $a \equiv a_0 \pmod{p}$.

We apply Hensel's lemma to $f(x) = x^{p-1} - 1$ for $p > 2$. Since $f(x) \equiv 0 \pmod{p}$ has $p - 1$ solutions in Z and conditions for Hensel,s lemma are satisfied, each of them can be lifted to a solution of $f(x) = 0$ in Q_p. In other words, for each i, $1 \leq i \leq p - 1$, we have a number $w(i) \in Z_p$, called the Teichmuller representative of the corresponding residue class mod p, such that

$$w(i) \equiv i \pmod{p}$$

with

$$w(i)^{p-1} = 1.$$

This allows us to define the so called Teichmuller character which is the multiplicative map from $(Z/pZ)^* \rightarrow Z_p$ given by $x \rightarrow w(x)$. We also note that every

$$x \in Z_p^* = \{x \in Z_p \ : \ |x|_p = 1\}$$

can be written uniquely as $x = w(x) < x >$ with $< x > \in 1 + pZ_p$. For $p = 2$, slight change has to be made.

It should be mentioned that Hensel's lemma implies that Q_p is not algebraically closed. In fact, a deeper analysis shows that, if we replace Q_p by its algebraic closure $\overline{Q}_p$ (by the usual method of extending norms from base field to finite extensions), $\overline{Q}_p$ fails to be complete with respect to that extended norm. Therefore, sometimes it is necessary to consider C_p, the completion of

$\overline{Q}_p$. The norm on $\overline{Q}_p$ can be extended to C_p by a routine exercise. C_p turns out to be complete, algebraically closed and $\overline{Q}_p$ is dense in C_p.

Fortunately, the concepts of convergence of series and power series in Q_p which we discussed earlier can be extended to C_p (or for that matter to $\overline{Q}_p$ or other extensions of Q_p). For example, the p-adic logarithm defined by

$$\log_p(1+x) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$$

is well-defined for $|x|_p < 1$ in C_p. However, the brilliant work of Iwasawa had shown how to extend p-adic log to all of $C_p^* = C_p - \{0\}$. This construction of Iwasawa rests on the crucial fact that any element x in C_p^* can be written in the form

$$p^r \; w(x_1) \; < x_1 >$$

where $|x_1|_p = 1$ and $|x_1 - 1|_p < 1$. Then we define for $x \in C_p^*$, as

$$\log x = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}\,(< x_1 > -1)^n}{n}$$

after first setting logarithms of roots of unity to be 0.

Observing that we do have the notion of derivative of a continuous function f with respect to p-adic metric ;

$$f'(x) = \lim_{n\to\infty} \frac{f(x+p^n) - f(x)}{p^n}$$

provided the limit exists. It is easy to see, for example, that the derivative of

x^n is nx^{n-1}. More importantly for us, it turns out that the p-adic logarithm is locally analytic in C_p^* i.e., it can be expanded into a power series in sufficiently small neighbourhood of each point of C_p^*. Differentiating this series term by term we see that

$$\left(\log_p(x)\right)' = \frac{1}{x}$$

in C_p^*.

3.4 p-adic Gamma Function Γ_p

We now discuss the p-adic gamma function. The idea is to have a p-adic function which mimics the essential properties of the classical gamma function. One way is to extend the function $n \to n!$ from Z to Z_p p-adically. However such an extension is not possible because $|n|_p \to 0$ as powers of p increase as n increases. Hence our approach needs a little modification. Consider a product

$$\prod_{1 \le j < n,\, p \nmid j} j.$$

Then it can be shown that

$$\prod_{a \le j < a+p^v, p \nmid} j \equiv -1 \pmod{p^v} \quad a, v \in Z, \quad v \ge 1.$$

This means that the function

$$f(n) := (-1)^n \prod_{1 \le j < n, p \nmid j} j \quad (n \ge 2).$$

from $N - \{0,1\}$ to Z is uniformly continuous with respect to the p-adic topology and hence it can be extended to a unique continuous function from Z_p to Z_p. Such an extension is possible as Z is dense in Z_p.

The resultant function on Z_p is called the (Morita) p-adic gamma function, Γ_p. Thus

$$\Gamma_p : Z_p \to Z_p$$

is a continuous function that extends

$$f(n) := (-1)^n \prod_{1 \le j \le n, p \nmid j} j \quad (n \ge 2)$$

.

By definition, this gamma function takes its values in the clopen subset Z_p^* of Z_p and it depends on the prime p.

We now collect the important properties of this p-adic function.
By definition $f(n) = \Gamma_p(n)$ if n is a rational integer. So

$$\Gamma_p(2) = 1, \quad \Gamma_p(3) = -2,$$

$$\Gamma_p(n+1) = \begin{cases} n! & \text{if } n\, is odd,\ n \le p-1 \\ -n! & \text{if } n\, is even,\ n \le p-1 \end{cases} \tag{1}$$

From definition it also follows that $\Gamma_p(n) \in Z_p^*$ is given by

$$\Gamma_p(n+1) = \frac{(-1)^{n+1} n!}{\prod_{1 \le kp \le n} kp} = \frac{(-1)^{n+1} n!}{[n/p]! p^{[n/p]}} \tag{2}$$

where $n \ge 2$. Again,

$$\Gamma_p(n+1) = \begin{cases} -n\Gamma_p(n) & \text{if } p \nmid n \\ -\Gamma_p(n) & \text{if } p|n \end{cases} \tag{3}$$

and by continuity,

$$\Gamma_p(x+1) = \begin{cases} -x\Gamma_p(x) & \text{if } x \in Z_p^* \\ -\Gamma_p(x) & \text{if } x \in pZ_p \end{cases} \tag{4}$$

It is convenient to introduce a function h_p:

$$h_p(x) = \begin{cases} -x & \text{if } x \in Z_p^* \ (|x| = 1) \\ -1 & \text{if } x \in pZ_p \ (|x| < 1) \end{cases}$$

so that we can write

$$\Gamma_p(x+1) = h_p \cdot \Gamma_p(x) \ (x \in Z_p) \tag{5}$$

.

This functional equation can be used backwards to compute the values $\Gamma_p(1)$ and $\Gamma_p(0)$ from $\Gamma_p(2) = 1$. Thus we get $\Gamma_p(0) = 1$.This also follows by continuity of this function. By the preceeding proposition we have

$$\Gamma_p(p^n) = -\prod_{1 \le j \le p^n, p \nmid j} j \equiv +1 \pmod{p^n} \tag{6}$$

;

hence $\Gamma_p(p^n) \to 1$ as $n \to \infty$.

Moreover

$$\Gamma_p(0) = 1,\ \Gamma_p(1) = -1,\ \Gamma_p(2) = 1, \tag{7}$$

$$\Gamma_p(n+1) = (-1)^{n+1} n! \ \ (1 \leq n < p) \tag{8}$$

$$\Gamma_p(a + mp^v) \equiv \Gamma_p(a) \pmod{p^v} \tag{9}$$

$$|\Gamma_p(x)| = 1 \tag{10}$$

$$|\Gamma_p(x) - \Gamma_p(y)| \leq |x - y|,\ \ |\Gamma_p(x) - 1| \leq |x|. \tag{11}$$

$$\Gamma_p(x+1) = h_p(x)\Gamma_p(x). \leq \tag{12}$$

$$\Gamma_p(x) \cdot \Gamma_p(1-x) = (-1)^{R(x)}, \leq \tag{13}$$

where $R(x) \in \{1, 2, \cdots, p\}$, $R(x) \equiv x \pmod{p}$. (11) follows from (9) by continuity. For (13), let $f(x) = \Gamma_p(x) \cdot \Gamma_p(1-x)$. We have

$f(x+1) = h_p(x)\Gamma_p(x) \cdot \Gamma_p(-x)$,

and since $\Gamma_p(-x) = \Gamma_p(1-x)/h_p(x)$,

$f(x+1) = \epsilon(x) \cdot f(x),\ \epsilon(x) = h_p(x)/h_p(-x)$.

Now,

$$\epsilon(x) = \begin{cases} -1 & \text{if } |x| = 1 \\ +1 & \text{if } |x| < 1 \end{cases}$$

.

Take for x an integer n and iterate,

$$f(n+1) = \epsilon(n) \cdot f(n) = \cdots = (-1)^k f(1),$$

with an exponent k equal to the number of integers $j \leq n$ prime to p. Since the number of integers $j \leq n$ divisible by p is $[n/p]$, this exponent k is $n - [n/p]$. Hence

$$f(n+1) = \Gamma_p(n+1) \cdot \Gamma_p(-n) = (-1)^{n-[n/p]} \cdot \underbrace{\Gamma_p(1)\Gamma_p(0)}_{-1} = (-1)^{n+1-[n/p]}.$$

To find a formula given in (13), let $x = m = n+1$ (integer), whence $1 - m = -n$ and $\Gamma_p(m) \cdot \Gamma_p(1-m) = \Gamma_p(n+1) \cdot \Gamma_p(-n) = (-1)^{n+1-[n/p]}$.

With the expansion of the integer n in base p,

$$n = n_0 + n_1 p + \cdots = n_0 + p[\tfrac{n}{p}]$$

we infer that

$$n - [\tfrac{n}{p}] = n_0 + (p-1)[\tfrac{n}{p}].$$

Since $p - 1$ is even, this proves that $n - [n/p]$ has the same parity as n_0:

$$(-1)^{n+1-[n/p]} = (-1)^{n_0+1}.$$

Since $m = n + 1 \equiv n_0 + 1 \pmod{p}$ and $n_0 + 1$ is in $\{1, 2, \cdots, p\}$, we have $R(m) = n_0 + 1$, and the formula is proved for integral values $x = m$ of the variable. By density and continuity, it remains true for all $x \in Z_p$.

The classical Gamma function satisfies the Legendre relation

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z},$$

which implies for $z = 1/2$

$$\Gamma(\frac{1}{2})^2 = \pi, \ \Gamma(\frac{1}{2}) = \sqrt{\pi}.$$

Hence we can say that in Q_p, an analogue of the number π could be taken as $\Gamma_p(\frac{1}{2})^2 = (-1)^{(p+1)/2}$. In particular, if $p \equiv 1 \pmod 4$, $\Gamma_p(\frac{1}{2}) = \sqrt{-1}$ is a canonical square root of -1 in Q_p. This canonical imaginary unit can be identified easily. In the case $p \equiv 1 \pmod 4$, the Wilson congruence

$$(p-1)! \equiv (\tfrac{p-1}{2})!^2 \equiv -1 \pmod p$$

shows that$(\frac{p-1}{2})!$ mod p is a square root of -1. Since $(p+1)/2 \equiv \frac{1}{2} \pmod p$, property (11) gives

$$\Gamma_p(\tfrac{1}{2}) \equiv \Gamma_p((p+1)/2) = (-1)^{(p+1)/2}((p-1)/2)! \equiv -((p-1)/2)! \pmod p.$$

Chapter 4

Congruences For Binomial Coefficients Revisited

4.1 Introduction

This last chapter is devoted to certain congruences whose proofs demand concepts and techniques from p-adic analysis. They range from mean value theorems to properties of p-adic gamma function and Gross-Koblitz formula for Gauss sums. Most of the basic material needed from p-adic analysis have been covered in the last chapter. We begin by looking at a congruence of binomial coefficients which turns out to be a consequence of the p-adic analogue of the mean value theorem of real analysis. Its generalisation, namely Kazandzidis congruence, however needs p-adic gammâ function and its logarithm. We have followed Robert [18] for this material. The last part of

the chapter reviews the fascinating paper of Chowla, Dwork and Evans [5]. This paper deals with the mod p^2 determination of the binomial coefficient $\binom{(p-1)/2}{(p-1)/4}$. As in the proof of Kazandzidis congruence, p-adic gamma function is required. However deep results like Gross-Koblitz formula for Gauss sum are also needed. It is interesting to note that Fermat quotient does appear in the proof at a crucial stage.

4.2 Congruences for the binomial coefficient $\binom{pn}{pk}$

To establish the first of these congruences, we need to look at the p-adic analogue of the mean value theorem. Consider a formal power series

$$\sum_{n=0}^{\infty} a_n x^n$$

over Q_p with the restriction that $|a_n|_p \to 0$; such series will be referred to as restricted power series. A "norm" can be associated with such a restricted power series $f(x) = \sum a_n x^n$ by declaring

$$\| f \| = sup_{n \geq 0} |a_n|_p.$$

Note that the "norm"

$$\| f' \| = sup_{n \geq 0} |na_n|_p \leq sup |a_n|_p = \| f \|$$

Given a restricted power series

$$f(x) = \sum_{n=0}^{\infty} a_n x^n,$$

we can associate a function f on the unit ball

$$\{x \in Q_p : |x|_p \leq 1\}$$

given by

$$f(t) = \sum_{t=0}^{\infty} a_t t^n.$$

The mean value theorem then states that

$$|f(t+h) - f(t)|_p \leq |h|_p \cdot \| f' \|$$

for $|t|_p \leq 1$, $|t+h|_p \leq 1$ with $|h|_p \leq p^{-1/(p-1)}$.

However, for our purpose we need a slightly more general estimate. Let K be a Banach space (e.g., a finite dimensional vector space) over Q_p such that the extended "norm" $\| \ \|$ is again non-archimedean on K. Now assume that

$$f(x) = \sum a_n x^n$$

is a restricted power series with coefficients in K. Then we consider

$$f : \{x \in Q_p : |x|_p \leq 1\} \rightarrow K$$

by

$$f(t) = \sum a_n t^n.$$

A variant of the mean value theorem gives an estimate of the "norm" of such function; the norm of f is calculated by "norms" of element of K,

$$\| f \| = sup_{n \geq 0} \| a_n \| .$$

The relevant result is

$$\| f(t+h) - f(t) \| \leq |h| \cdot \| f' \|$$

for all

$$t,\ h\ \in \{x \in Q_p\ :\ |x|_p \leq 1\}$$

and

$$|h| < p^{-\frac{1}{p-1}}$$

We apply this estimate to some appropriate function f. For us, f will be a "vector-valued" function with values in the finite dimensional vector space of polynomials of degree less than or equal to some fixed integer with coefficients in Q_p. For extension of the p-adic norm from Q_p to a finite dimensional vector space over Q_p, see Koblitz [13]. Let f, g be polynomials, to begin with, with integral coefficients given by

$$(1+x)^p\ =\ 1 + p \cdot g(x) + x^p$$

and

$$f(t) = (1 + t\, g(x) + x^p)^n$$

so that $t \mapsto f(t)$ is a function from the unit disc in Q_p to K where K is the Banach space of all polynomials over Q_p of degree atmost np. The estimate (2) gives us a bound of the "norm" of $f(p) - f(0)$. However

$$f(0) = (1 + x^p)^n$$

$$f(p) = (1 + pg(x) + x^p)^n \; = ((1 + x)^p)^n \; = (1 + x)^{pn}$$

so that

$$f(p) - f(0) = (1 + x)^{pn} - (1 + x^p)^n = \sum_j \binom{pn}{j} x^j - \sum \binom{n}{k} x^{pk}$$

But $\| f' \| \leq |n|_p$ and it follows that $\| f(p) - f(0) \| \leq |np|_p$. The last "norm" $\| \|$ is the sup norm of the Banach space K and hence all the coefficients of the polynomial $f(p) - f(0)$ must be bounded by $|np|_p$. In particular, looking at the coefficient of x^{pk} we see that

$$\left| \binom{pn}{pk} - \binom{n}{k} \right|_p < |np|_p$$

Thus

(1) $$\binom{pn}{pk} - \binom{n}{k} \in npZ_p$$

yielding the following congruence

4.2.1 Theorem. *Let p be a prime, and n, k positive integers with $k \leq n$. Then*

$$\binom{pn}{pk} \equiv \binom{n}{k} \pmod{pnZ_p} \tag{2}$$

Note that Kazandzidis congruence generalises theorem 1.7.3

The attempt to generalise the congruence

$$\binom{pn}{pk} \equiv \binom{n}{k} \pmod{pnZ_p}$$

rests on the observation that the quotient

$$\binom{pn}{pk} \Big/ \binom{n}{k}$$

can be expressed in terms of p-adic gamma function, namely

$$\binom{pn}{pk} \Big/ \binom{n}{k} = \frac{\Gamma_p(pn)}{\Gamma_p(pk)\Gamma_p(pl)} \tag{3}$$

where $k + l = n$.

Since the left hand side is a p-adic unit, (as the quotient belongs to $1 + pZ_p$), it follows that to generalise the congruence (1) one has to show that the quotient actually belongs to $1 + p^r Z_p$ for $r > 1$. This requires the p-adic logarithm.

The typical term on the right hand side of (3) is $\Gamma_p(px)$. Since $|\Gamma_p(px) - 1|_p < |x|_p$, and for

$$|y-1|_p < p^{-1/(p-1)}, \quad |\log y|_p = |y-1|_p,$$

it follows that

$$\left|\frac{\Gamma_p(px+py)}{\Gamma_p(px)\Gamma_p(py)} - 1\right|_p = \left|\log \frac{\Gamma_p(px+py)}{\Gamma_p(px)\Gamma_p(py)}\right| \tag{4}$$

for $x, y \in Z_p$. (To compare with (3) put $x + y = n$, $x = k$ and $y = l$). Finally, therefore one considers the function $f(x) = \log \Gamma_p(px)$, so that the right hand side of (4) is just $|f(x+y) - f(x) - f(y)|$. The generalisation that was sought, then follows once it is shown that

$$|f(x+y) - f(x) - f(y)| \leq |p^3 xy(x+y)|. \tag{5}$$

To show this, one needs to first observe that $f(x)$ can be shown to be a restricted power series, and that $f(x)$ is an odd function. Then careful determination of the coefficient of $f(x)$ yields (5). Once (5) is established, we easily obtain Kazandzidis congruence, namely

4.2.2 Theorem. *For all primes $p \geq 5$, and positive integers n, k, $(k \leq n)$*

$$\binom{pm}{pk} \equiv \binom{n}{k} \pmod{p^3 nk(n-k)\binom{n}{k} Z_p}.$$

4.3 The residue of $\binom{(p-1)/2}{(p-1)/4}$ mod p^2

For a prime p, if $p = 4n+1$, then it is known that $p = a^2 + b^2$ where $a \equiv 1 \pmod 4$. A famous congruence of Gauss states that

$$2a \equiv \binom{2n}{n} \pmod p.$$

Since $p = 4n+1$, it can also be stated as

$$A \equiv 2a \pmod p$$

where A is the binomial coefficient $\binom{(p-1)/2}{(p-1)/4}$. Chowla, Dwork and Evans [5] used Gross-Koblitz formula for Gauss sums and Diamond's formula [8] to derive the following generalisation proposed by F. Beukers:

$$A \equiv \left(1 + \frac{2^{p-1}-1}{2}\right)\left(2a - \frac{p}{2a}\right) \pmod{p^2} \tag{1}$$

We shall be working in C_p, the completion of Q_p with $|\ |$ as the extended valuation on C_p. Recall that Iwasawa's log is defined on C_p^* with series expansion

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

for $|x| < 1$ in C_p^*.

Also recall that the p-adic gamma function Γ_p is locally analytic on R, where R is the disjoint union of the following disks

$$R = \bigcup_{t=0}^{p-1} D(-t, \rho^-).$$

where

$$1/\rho = p^{\frac{1}{p}+\frac{1}{p-1}} < p$$

and

$$D(-t,\rho) = \{x \in C_p | \ |x+t| < \rho\}.$$

For $x \in D(-t,\rho^-)$, we let

(2) $$Rep(-x) = t \quad (0 \leq t \leq p-1)$$

Note that R contains Z_p as a proper subset. We have the following properties of Γ_p:

(3) $$\Gamma_p(0) = 1$$

(4) $$\Gamma_p(1+x)/\Gamma_p(x) = \begin{cases} -x & \text{if } |X| = 1 \\ -1 & \text{if } |x| < 1 \end{cases}$$

(5) $$|\Gamma_p(x)| = 1$$

$$\Gamma_p(x)\Gamma_p(1-x) = -(-1)^t$$

if $x \in D(-t, 1/\rho), t = 0, 1, \cdots, p-1$(6)

(7) $$\Gamma_p^{(n)}(x) \in Q_p$$

for all $x \in Z_p, n \in N$.

Diamond's formula [8] for the values of the logarithmic derivative Γ_p'/Γ_p at the elements of $Z_p \cap Q$ will also be needed. It says that for $a \in Q \cap Z_p$, $t = Rep(-a)$, if we let a' be defined by

$$pa' - a = t$$

then $G = \Gamma_p'/\Gamma_p$ can be evaluated at $x = a$ by

(8) $$G(a) - G(1) = \sum_{z^d=1,\, z\neq 1} ((z^{da} - 1) - p^{-1}(z^{da'} - 1)) \log(1 - z),$$

where the sum is over all the d^{th} roots of unity except $z = 1$ and where d is the denominator of a.

We also need to consider a variant of Gauss sum. Recall that for $\bar{t} \in F_p$, we have a lifting $t = Teich\,\bar{t}$ to Z_p such that all such lifting are $(p-1)^{th}$ roots of unity. Let ξ_p be the p^{th} root of unity (in the Galois extension $Q(\xi_p)$ of Q) such that

$$\xi_p \equiv 1 + \pi \pmod{\pi^2}$$

with $\pi \in C_p$ s.t. $\pi^{p-1} = -p$. (such a choice is possible by a result of Dwork). We may then define a nontrivial additive character θ, on F_p by

$$\theta(\bar{t}) = \xi_p^t,$$

where t is the Teichmuller representative of $\bar{t}$ in Z_p. For $j \in Z/(p-1)Z$ we let the Gauss sum

$$g(j) = -\sum \xi_p^t t^{-j} \tag{9}$$

where the sum is over all the $(p-1)st$ roots of unity t. Observe that $g(j)$ is an element of $Q(\xi_p, \xi_{p-1})$. As usual, conjugate of g is defined by

$$\text{conj } g(j) = -\sum \xi_p^{-t} t^j = g(j)(-1)^j.$$

so that

$$\text{conj } g(j)g(j) = p.$$

By the Gross Koblitz formula for such Gauss sums, we get, for $0 \leq j \leq p-1$ then

$$g(j) = \pi^j \, \Gamma_p\left(\frac{j}{p-1}\right) \tag{10}$$

We introduce

$$B_0 = -\Gamma_p(1/4)^2 \Gamma_p(1/2).$$

which by the formulas listed in the last chapter is related to the binomial coefficient. By (10) we can identify B_0 with

$$B = p^{-1} g\left(\tfrac{p-1}{4}\right)^2 g\left(\tfrac{p-1}{2}\right).$$

By a result of Hasse, it is known that

$$B = a + ib, \quad a, b \in Z.$$

where

$$p = a^2 + b^2,$$

$$a \equiv 1 \pmod 4.$$

Thus, our identification allows us to obtain

$$B_0 + \frac{p}{B_0} = 2a \tag{11}$$

as $B \cdot conj\, B = p$.

After these preliminaries, we come to the proof of the actual result. First write A in terms of Γ_p. If $0 \leq n \leq p-1$, then from (3) and (4)

$$n! = (-1)^{n+1}\Gamma_p(1+n).$$

Now, Rep-$(1+n) = p - 1 - n$ and hence

$$n! = 1/\Gamma_p(-n) \tag{12},$$

for $0 \leq n \leq p-1$

Therefore,

$$A = \left(\frac{p-1}{2}\right)! \Big/ \left(\frac{p-1}{4}\right)!^2 = \Gamma_p\left(\frac{1-p}{4}\right)^2 \Big/ \Gamma_p\left(\frac{1-p}{2}\right) \tag{13}$$

If $x_0 \in R$ and $|x| < \rho$, then by Taylor's theorem,

$$\Gamma_p(x_0 + z) = \sum_{n=0}^{\infty} a_n z^n$$

so that Cauchy's inequality and (5) give

$$|a_n|\rho^n \leq 1, \quad \forall n \in N,$$

$$|a_0| = |\Gamma_p(x_0)| = 1.$$

In particular if $|z| \leq |p|$ then

$$|a_n z^n| \leq (|p|/\rho)^n = |p|^{n(1-(1/p)-(1/(p-1)))}.$$

If $x_0 \in Z_p$, then by (7) $a_n \in Q_p$, i.e.,

$$ord_p(a_n) \in Z.$$

and so there is an n such that

$$a_n z^n \equiv 0 \pmod{p^{c_n}},$$

with c_n , the smallest integer $\geq n\,(1 - 1/p - 1/(p-1))$.
For $n \geq 2$ we have

$$c_n \geq c_2 \geq 2\,(1 - 1/p - 1/(p-1)))\,.$$

If $p \geq 5$,then $c_2 \geq 2$.

This proves for $p \geq 5$,

4.3.1 Proposition. *For $x_0 \in Z_p$, $|z| \leq |p|$ we have*

$$\Gamma_p(x_0 + z) \equiv \Gamma_p(x_0) + z\Gamma_p'(x_0) \pmod{p^2}.$$

Using this in (13) and taking $A_0 = \Gamma_p(1/4)^2/\Gamma_p(1/2)$, we get

$$A \equiv \frac{\left(\Gamma_p(1/4) - \frac{p}{4}\Gamma_p'(1/4)\right)^2}{\Gamma_p(1/2) - \frac{p}{2}\Gamma_p'(1/2)} \pmod{p^2}$$

$$\equiv \frac{\Gamma_p(1/4)^2}{\Gamma_p(1/2)} \left(\frac{1 - \frac{p\Gamma_p'(1/4)}{2\Gamma_p(1/4)}}{1 - \frac{p\Gamma_p'(1/2)}{2\Gamma_p(1/2)}} \right) \pmod{p^2}$$

$$\equiv A_0 \left(1 + \frac{p}{2}(G(1/2) - G(1/4))\right) \pmod{p^2}.$$

On the other hand, from (8)

$$\begin{aligned} G(1/2) - G(1/4) &= ((-1-1) - p^{-1}(-1-1))\log(1-(-1)) - [(-1-1) \\ &\quad -p^{-1}(-1-1))\log(1-(-1)) + ((i-1) - p^{-1}(i-1))\log(1-i) + ((-i-1) \\ &\quad -p^{-1}(-i-1))\log(-i-1)] \\ &= 1 - \tfrac{1}{p}\log 2 \;= \tfrac{1}{p}\log 2^{p-1}, \end{aligned}$$

since $\log(1-i)/(1+i) = 0$ (Iwasawa's construction). From the power series expansion of $\log 2^{p-1}$, we get

$$\log 2^{p-1} \equiv 2^{p-1} - 1 \pmod{p^2}.$$

Also, it follows easily from (6) that

$$\Gamma_p(1/2)^2 = -(-1)^{(p-1)/2} = -1$$

and so $A_0 = B_0$.

Thus we have

$$A \equiv B_0 \left(1 + \frac{2^{p-1} - 1}{2}\right) \pmod{p^2}$$

Thus our main congruence will be proved if we can show that

$$B_0 \equiv 2a - p/(2a) \pmod{p^2}$$

It follows from (11) that $B_0 + conj\, B_0 = 2a$. Hence B_0 is the fixed point of the function

$$x \;\to\; 2a - p/x.$$

If

$$B_0 = \sum_{k\geq 0} a_k p^k$$

is the p-adic expansion of B_0, then

$$\sum_{k\geq 0} a_k p^k = 2a - p/B_0$$

implies

$$\left(\sum_{k\geq 0} a_k p^k\right)^2 = 2a \sum_{k\geq 0} a_k p^k - p$$

Taking this relation mod p and p^2 we get

$$B_0 \equiv 2a - \tfrac{p}{2a} \pmod{p^2}.$$

This completes the proof.

Bibliography

[1] Chowla. S. , *A proof of a theorem of Wolstenholme*, Math.Student 1(1933), 106 – 107.

[2] Chowla.S. , *A generalisation of Wolstenholme's Theorem*, Math.Student 1, (1933), 140 – 141.

[3] Chowla.S. , *Leudesdorf's generalisation of Wolstenholme's Theorem*, J.London Math. Soc 9(1934)246.

[4] Chowla.S. , *A generalisation of a theorem of Wolstenholme*, J. London Math. Student.Soc. 5 (1930), 154 – 160.

[5] Chowla.S.,Dwork.B,Evans.R. , *On the mod p^2 determination of* $\binom{(p-1)/2}{(p-1)/4}$, J. Number theory 24(1986) 188 – 196.

[6] Chowla S. , *A new proof of Von Staudt's theorem*,J.Indian Math.Soc. (notes and Questions)16(1926), 145 – 146.

[7] Dilcher.K. , *An extension of Fermat's little theorem and congruences for primes*, Amer.Math.Monthly 104(2000), 936 – 940.

[8] Diamond.J. , *The p – adic log gamma and p – adic Euler constants*, trans. Amer.Math. Soc. 233(1977), 321 – 337.

[9] Guy.R.(Editor) , *Reviews in Number Theory*,(1973–1983) Amer. Math.Soc.Providence,

RI, 1984.

[10] Hardy G.H. and Wright E.M. , *An Introduction to Number Theory*, Oxford Univ. Press (1959).

[11] Ireland K.M.R. , *A Classical Introduction to Modern Number Theory* GTM 84 Springer-Verlag New York Heidelberg Berlin.

[12] Jothilingam P. , *Generalisation of Eisenstein's congruence*, Acta Math.Hung. 46(1985) 265 – 267.

[13] Koblitz N. , *p – adic numbers, p – adic, analysis and Zeta – Functions*, GTM 58 Springer-Verlag New York Heidelberg Berlin.

[14] Kohnen W. , *A simple congruence modulo p*, Amer Math Monthly Vol 104, 5(may, 1997).

[15] Ram Murty M. , *Introduction to p – adic analytic number theory*, Lecture Note,Mehta Research Institute,Allahabad.

[16] Ribenboim P. , *The Book of Prime Number Records* Second Edition, Springer-Verlag New York Berlin Heidelberg London Paris Tokyo.

[17] Riordan J. , *Combinatorial Identities*, John Wiley and Sons, Inc. New York. Sydney.

[18] Robert A. M. , *A Course in p – adic analysis*, GTM Springer-Verlag

[19] Sun Z. W. , *A congruence for primes*, Proc. Of the Amer.Math.Soc. 123,No.5 (1995) 1341 – 1346.

[20] Washington L.C. , *Introduction to Cyclotomic Fields* GTM 83 springer-Verlag New York Heidelberg Berlin.

103327

NEHU LIBRARY
Acc. No.
Acc. No.
Date 28-3-05
Tra... by...