ANALOGUES OF THE BINOMIAL COEFFICIENT THEOREMS OF GAUSS AND JACOBI

by

Abdullah Al-Shaghay

Submitted in partial fulfillment of the
requirements for the degree of
Master of Science

at

Dalhousie University
Halifax, Nova Scotia
March 2014

Table of Contents

List of Tables

Abstract

Two of the more well known congruences for binomial coefficients modulo p, due to Gauss and Jacobi, are related to the representation of an odd prime (or an integer multiple of the odd prime) p as a sum of two squares (or an integer linear combination of two squares). These two congruences, along with many others, have been extended to analogues modulo p^2 and are well documented in [1]. More recently, J. Cosgrave and K. Dilcher, in [7] and [9], have extended the congruences of Gauss and Jacobi and a related one due to Hudson and Williams, to analogues modulo p^3. In this thesis we discuss their methods as well as the potential of applying them to similar congruences found in [1].

List of Abbreviations and Symbols Used

In what follows, and throughout this thesis, n and r always denote a positive integer, p a prime, and q a power of a prime.

Notation	Description
$a \equiv b \pmod{n}$	a is congruent to b modulo n; that is, $b - a = kn$ for some integer k.
$a \not\equiv b \pmod{n}$	a is not congruent to b modulo n; that is, $b - a \neq kn$ for any integer k.
$\gcd(a, b)$	Greatest common divisor of a and b.
$\binom{n}{k}$	Binomial coefficient defined by $\frac{n!}{(n-k)!k!}$.
$q_p(m)$	Fermat quotient defined by $\frac{m^{p-1}-1}{p}$.
E_n	The nth Euler number.
C_n	The nth Catalan number defined by $\frac{1}{n+1}\binom{2n}{n}$.
$B_n(x)$	The nth Bernoulli polynomial.
B_n	The nth Bernoulli number.
$N_n!$	Gauss factorial of N modulo n.
$\mathbb{Q}$	Field of rational numbers.
$\mathbb{Z}$	Ring of integers.
$\mathbb{Q}_p$	Field of p-adic numbers.
$\mathbb{Z}_p$	Ring of p-adic integers in $\mathbb{Q}_p$.
$\mathbb{Z}_p^*$	Group of units in $\mathbb{Z}_p$.
$\mathbb{F}_q$	Finite field with q elements.
$\mathbb{F}_q^*$	Group of units in $\mathbb{F}_q$.
$G_r(\beta, \chi)$	Gauss sum for the element β and the character χ.
$J_r(\chi, \psi)$	Jacobi sum for the characters χ and ψ.
$\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$	The smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $\alpha_1, \ldots, \alpha_n$.
$\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$	The smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and $\alpha_1, \ldots, \alpha_n$.
$\left(\frac{a}{p}\right)$	Legendre symbol of a and p defined for integers a and odd primes p for which $p \nmid a$ to be 1 if $x^2 \equiv a \pmod{p}$ for some x and -1 otherwise.

Notation	Description
$a \mid b$	a divides b; that is, $b = ak$ for some integer k.
$a \nmid b$	a does not divide b, that is, $b \neq ak$ for any integer k.
$\mathrm{ind}_g a$	Index of a base g modulo p defined to be the least nonnegative integer k such that $g^k \equiv a \pmod{p}$.
$\mathfrak{p}$	A prime ideal in the given ring of integers that divides the prime p.
$m \equiv n \pmod{\mathfrak{a}}$	m is congruent to n modulo the ideal $\mathfrak{a}$; that is, the element $m + (-n)$ belongs to the ideal $\mathfrak{a}$.

Acknowledgements

I would like to especially thank my supervisor, Dr. Karl Dilcher, for everything he has done for me. He is a wonderful teacher, supervisor, and mentor. This thesis would not have been possible without his assistance, patience, and understanding.

I would like to thank Dr. Rob Noble and Dr. Keith Johnson for taking the time to read and comment on my thesis. I really value and respect both of your opinions; all of your help is greatly appreciated.

I would like to thank my family and friends for their continued support throughout my education. They have always been a great source of encouragement and advice.

Finally, I would like to thank the Department of Mathematics and Statistics at Dalhousie University for all of their support. The faculty, administrative staff, and other students have made my experience very enjoyable.

Chapter 1

Introduction

Many mathematicians were interested in the problem of determining the value of binomial coefficients modulo an odd prime p; among them were C. Gauss, C. Jacobi, E. Lehmer, A.Whiteman, L. von Schrutlea, R. Hudson, and K. Williams. In the late 1980s, a number of authors began considering the problem of determining the value of binomial coefficients modulo p^2 rather than modulo p [1, Chapter 9]. In this thesis, we will be concerned with determining the value of binomial coefficients modulo p^3.

1.1 The Theorems of Gauss and Jacobi

One of the earliest and better known congruences for binomial coefficients, due to Gauss (1828), is related to the representation of an odd prime p (congruent to 1 modulo 4) as a sum of two squares.

Let $p \equiv 1 \pmod 4$ be prime. It is well known that such primes p admit a representation as a sum of two integer squares. But if we consider such a representation $p = a^2 + b^2$ for integers a and b modulo 4, and use the fact that the only squares modulo 4 are 0 and 1, we can conclude that exactly one of a^2, b^2 is congruent to 1 modulo 4 (and the other is congruent to 0 modulo 4). Without loss of generality, we may then suppose that $a^2 \equiv 1 \pmod 4$ so that $a \equiv \pm 1 \pmod 4$. Finally, by switching the sign of a, if necessary, we can assume that $a \equiv 1 \pmod 4$. The following notation that will be used in several of the following results therefore makes sense.

$$p = a^2 + b^2 \equiv 1 \pmod 4 \quad \text{where } a \equiv 1 \pmod 4 \tag{1.1}$$

Theorem 1.1. *Let p, a, b satisfy* (1.1)*. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p.$$

This congruence was discovered by Gauss as a result of his work on quartic and biquadratic reciprocity (see, e.g., [25, Section 6.2]).

Beukers, in [2], conjectured the following modulo p^2 extension of this congruence which was proven by Chowla, Dwork, and Evans in 1986 [4].

Theorem 1.2. *Let p, a, b satisfy* (1.1)*. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(1 + \frac{1}{2}pq_p(2)\right)\left(2a - \frac{p}{2a}\right) \pmod{p^2},$$

where $q_p(m)$ denotes the Fermat quotient, defined for integers m and odd primes $p \nmid m$ by

$$q_p(m) := \frac{m^{p-1} - 1}{p}.$$

More recently, Cosgrave and Dilcher [7] (2010) have extended this congruence to the following analogue modulo p^3.

Theorem 1.3. *Let p, a, b satisfy* (1.1)*. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(2a - \frac{p}{2a} - \frac{p^2}{8a^3}\right)\left(1 + \frac{1}{2}pq_p(2) + \frac{1}{8}p^2\left(2E_{p-3} - q_p(2)^2\right)\right) \pmod{p^3}.$$

Here E_{p-3} denotes the $(p-3)$rd Euler number, where the Euler numbers $E_n, n \geq 0$

are defined by the exponential generating function

$$\frac{1}{\cosh(x)} = \frac{2}{e^x + e^{-x}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} x^n.$$

Theorem 1.1 follows from an identity involving Jacobsthal sums while Theorem 1.2 was proved using the Gross-Koblitz formula along with a formula due to J. Diamond. Theorem 1.3, which is the main focus of this thesis, was proved using Gauss factorials, Morita's p-adic gamma function, a special case of the Gross-Koblitz formula, and congruences for certain finite sums modulo p and p^2.

In [7], the authors use a consequence of the Gross-Koblitz formula to relate a particular Jacobi sum to a quotient of values of Morita's p-adic Γ-function. Properties of Morita's p-adic Γ-function are then used, along with explicit evaluations of the Jacobi sum, to obtain Theorem 1.4 below.

Definition 1.1. *The Gauss factorial $N_n!$ is defined by*

$$N_n! = \prod_{\substack{1 \le j \le N \\ \gcd(j,n)=1}} j.$$

Definition 1.2. *The nth Catalan number, which is always an integer, is defined by*

$$C_n := \frac{1}{n+1}\binom{2n}{n}.$$

Theorem 1.4. *Let p, a, b satisfy* (1.1) *and $\alpha \ge 2$ be an integer. Then*

$$\begin{aligned}\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} &\equiv 2a - C_0\frac{p}{2a} - C_1\frac{p^2}{8a^3} - \ldots - C_{\alpha-2}\frac{p^\alpha - 1}{(2a)^{2\alpha-1}} \\ &= 2a - 2a\sum_{j=1}^{\alpha-1} \frac{1}{j}\binom{2j-2}{j-1}\left(\frac{p}{4a^2}\right) \pmod{p^\alpha}.\end{aligned}$$

The quotient on the left-hand side of this congruence strongly resembles a central

binomial coefficient and Theorem 1.1 is a direct consequence of Theorem 1.4. We will also see that Theorem 1.3 follows from Theorem 1.4.

Let $p \equiv 1 \pmod 3$ be prime. It is known that such primes p admit a representation as a sum of an integer square and 3 times an integer square. But if we consider such a representation $p = a^2 + 3b^2$ for integers a and b modulo 3, and use the fact that the only squares modulo 3 are 0 and 1, we can conclude that a^2 is congruent to 1 modulo 3. The congruence $a^2 \equiv 1 \pmod 3$ then implies that $a \equiv \pm 1 \pmod 3$. Finally, by switching the sign of a if necessary, we can assume that $a \equiv 1 \pmod 3$. It follows that, with $r = 2a$, $s = 2b$ we can represent $4p = r^2 + 3s^2$ with $r \equiv 1 \pmod 3$. The following notation that will be used in several of the later results therefore makes sense.

$$4p = r^2 + 3s^2 \equiv 1 \pmod 3 \quad \text{where } r \equiv 1 \pmod 3 \tag{1.2}$$

Similar to Gauss' theorem of 1828, Jacobi (1837) is credited for the following result.

Theorem 1.5. *Let p, r, s satisfy (1.2). Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p.$$

This congruence has been extended to the following analogue modulo p^2, independently by Evans and by Yeung; see [1, page 293] for both references and additional comments.

Theorem 1.6. *Let p, r, s satisfy (1.2). Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r + \frac{p}{r} \pmod{p^2}.$$

Similarly to how Cosgrave and Dilcher obtain their modulo p^3 analogue of Theorem 1.2 given by Theorem 1.3, they also obtain the following modulo p^3 analogue of

Theorem 1.6, appearing in [7].

Theorem 1.7. *Let p, r, s satisfy* (1.2)*. Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv \left(-r + \frac{p}{r} + \frac{p^2}{r^3}\right)\left(1 + \frac{1}{6}p^2 B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.$$

Here $B_{p-2}(x)$ denotes the $(p-2)$nd Bernoulli polynomial, where these polynomials, $B_n(x)$, $n \geq 0$ are defined by the exponential generating function

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} t^n.$$

1.2 The Theorem of Hudson and Williams

Similarly to the previous section, the following congruence is found in the work of Hudson and Williams [22].

Let $p \equiv 1 \pmod 6$ be prime. Then we also have that $p \equiv 1 \pmod 3$ and we may use the reasoning of the previous section to justify the following notation.

$$p = a_3^2 + 3b_3^2, \quad a_3 \equiv -1 \pmod 3 \tag{1.3}$$

$$4p = u_3^2 + 3v_3^2, \quad u_3 \equiv 1 \pmod 3 \tag{1.4}$$

Theorem 1.8. *Let $p \equiv 1 \pmod 6$ be a prime and a_3, b_3 as in* (1.3)*. Then we have*

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1} u_3 \equiv \begin{cases} 2(-1)^{\frac{p-1}{6}+1} a_3 & \pmod p \text{ if } b_3 \equiv 0 \pmod 3, \\ (-1)^{\frac{p-1}{6}}(a_3 + 3b_3) & \pmod p \text{ if } b_3 \equiv 1 \pmod 3, \\ (-1)^{\frac{p-1}{6}}(a_3 - 3b_3) & \pmod p \text{ if } b_3 \equiv 2 \pmod 3. \end{cases}$$

This congruence has been extended to the following analogue modulo p^2, as found in [1].

Theorem 1.9. *Let $p \equiv 1 \pmod 6$ and u_3 as in (1.4), then*

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1}\left(u_3 - \frac{p}{u_3}\right)\left(1 + \frac{2^p - 2}{3}\right) \pmod{p^2}.$$

In analogy with Theorem 1.4, J. Cosgrave and K. Dilcher obtained the following result (see [10]).

Theorem 1.10. *Let $p \equiv 1 \pmod 6$ and u_3 as in (1.4), then*

$$\frac{(\frac{p^\alpha-1}{3})_p!}{((\frac{p^\alpha-1}{6})_p!)^2} \equiv (-1)^{\frac{p-1}{6}+1}\left(u_3 + u_3\sum_{j=1}^{\alpha-1}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{u_3^2}\right)^j\right) \pmod{p^\alpha}.$$

1.3 Morley's Congruence

Another famous congruence involving binomial coefficients and prime numbers is due to Morley (1895). In [28], using DeMoivre's theorem, Morley proved the following.

Theorem 1.11. *For any prime $p \geq 5$,*

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \pmod{p^3}.$$

We note that when $p = 3$, the above congruence fails modulo 3^3 but holds modulo 3^2. For more comments on Morley's theorem as well as an interesting generalization, see [20]. This theorem was generalized to the following result by Carlitz in [3].

Theorem 1.12. *For any prime $p \geq 5$,*

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} + \frac{1}{12}p^3 B_{p-3} \pmod{p^4}.$$

Here B_{p-3} denotes the $(p-3)$rd Bernoulli number, where the Bernoulli numbers, $B_n, n \geq 0$ are defined by $B_n = B_n(0)$ with $B_n(x)$ denoting the nth Bernoulli polynomial.

1.4 Uses and Applications

Areas of Number Theory and Discrete Mathematics employ arithmetic properties of binomial coefficients. Congruence relations for binomial coefficients have been studied in the past by famous mathematicians such as Gauss, Kummer, Legendre, and Lucas.

One particular application of congruences of binomial coefficients is discussed in [26]; these types of congruences have extensive use in the study of Probabilistic Primality Testing. In Probabilistic Primality Testing there are many congruence relations that are always satisfied by prime numbers and are rarely satisfied by composite numbers. The following theorem is important for proving a large number of such congruence relations ([26]).

Theorem 1.13. *The positive integer n is prime if and only if*

$$\binom{n}{k} \equiv 0 \pmod{n}$$

for all k with $1 \leq k \leq n-1$.

On its own, this is not an efficient way to check primality since it requires the direct computation of binomial coefficients. However, this theorem is indirectly used to give effective probabilistic primality tests (see [26] for additional comments).

A celebrated theorem in Elementary Number Theory, due to Wilson, with the converse due to Lagrange, states the following.

Theorem 1.14. *A natural number $n > 1$ is prime if and only if*

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

Wilson primes are odd primes that do better than this last congruence; an odd prime p is called a *Wilson prime* if $(p-1)! \equiv -1 \pmod{p^2}$. The only known Wilson primes $p < 2 \times 10^{13}$ are $p = 5$, $p = 13$, and $p = 563$ ([11]). Congruences involving

binomial coefficients have also been used to help with the large-scale computations required in searching for Wilson primes as was done in [13]; see also [14, pp. 102ff.]

Finally in this section, we mention that Theorem 1.10 is an essential tool in the study of the multiplicative orders of certain Gauss factorials ([10]), namely those of the form $\left(\frac{n-1}{M}\right)_n! \pmod{n}$ for odd prime powers $n = p^\alpha$, $p \equiv 1 \pmod{M}$ and $M = 3$, and $M = 6$.

1.5 Goals

Similar to the theorems of Gauss, Jacobi, Hudson and Williams above, there exist many other congruence relations for binomial coefficients modulo an odd prime p. A large number of these results have been extended to modulo p^2 analogues, but very few of them have been extended beyond that to modulo higher powers of p, not even one step further to modulo p^3. We will use the methods outlined by Cosgrave and Dilcher in [7] to extend as many of the congruences found in [1] as we can to modulo p^3 analogues.

Chapter 2

Background

In this chapter we define the various mathematical objects that will be required later in this thesis. We also state, mostly without proofs, those results that will be essential later on.

2.1 Gauss Factorials

For the sake of completeness, we begin by repeating Definition 1.1:

Definition 2.1. *For positive integers N and n let $N_n!$ denote the product of all positive integers up to N that are relatively prime to n. That is,*

$$N_n! = \prod_{\substack{1 \le j \le N \\ \gcd(j,n)=1}} j.$$

In [6] these products are called Gauss factorials. In particular, $(n-1)_n! = n_n!$ is equal to the product of the units modulo n. In any finite abelian group, if one multiplies all of the elements of the group together, each element that isn't equal to its inverse will cancel with its (distinct) inverse in the product. We are therefore left with the product of the self-inversive elements of the group. Squaring this product therefore yields the identity element of the group and so either the group has odd order and the product is equal to the identity, or the group has even order and the product is equal to the identity or is equal to the unique element of the group having order 2. The case we are concerned with here is that where the group is equal to the multiplicative group of the integers modulo some n, having even order $\varphi(n)$ and unique element of order 2 equal to -1. We therefore obtain 1 or -1 as the value of

the product, but can we classify when each of these possibilities occurs? According to the following theorem of Gauss, it is completely determined by whether or not there exists a primitive root to the given modulus ([15, page 65]).

Theorem 2.1. *For any integer $n \geq 2$ we have*

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \text{for } n = 2, 4, p^\alpha, \text{ or } 2p^\alpha \\ 1 \pmod{n} & \text{otherwise,} \end{cases}$$

where p is an odd prime and α is a positive integer.

For further properties of the Gauss factorial, see [8].

2.2 Morita's p-adic Gamma Function

In [27], Morita constructs a p-adic analogue of the classical Γ-function. Morita's p-adic Γ-function satisfies some useful analogues to its classical counterpart, as will be seen in this section.

Define a function F on the non-negative integers by

$$F(0) := 1, \quad F(N) := (-1)^N \prod_{\substack{0<j<N \\ p \nmid j}} j \qquad (N \geq 1)$$

where $F(1)$ is interpreted as $F(1) = -1$, in accordance with the convention that the empty product equals 1.

Let $\mathbb{Q}_p$ denote the p-adic completion of the rationals $\mathbb{Q}$, and let $\mathbb{Z}_p$ denote the ring of p-adic integers in $\mathbb{Q}_p$. Denote the group of units in $\mathbb{Z}_p$ by $\mathbb{Z}_p^*$. Morita's p-adic gamma function is the function $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^*$ defined by

$$\Gamma_p(z) = \lim_{N \to z} F(N) \qquad (z \in \mathbb{Z}_p),$$

where N runs through any sequence of positive integers having p-adic limit equal to z.

For all $n \geq 0$, F is a well-defined (as the following lemma shows) function on $\mathbb{Z}/p^n\mathbb{Z}$, Consequently, F lifts to a well-defined map Γ_p on $\mathbb{Z}_p$.

Lemma 2.1. *If M, N, and n are non-negative integers, then*

$$M \equiv N \pmod{p^n} \qquad \textit{implies} \qquad F(M) \equiv F(N) \pmod{p^n}.$$

Proof. Let M, N, and n be as in the lemma. Without loss of generality, let $M < N$. $M \equiv N \pmod{p^n}$ implies $N - M = kp^n$ $(k \in \mathbb{Z})$. Using the definition of F, we see that $F(M) \not\equiv_p 0$. Thus $\frac{F(N)}{F(M)}$ makes sense and we have

$$\begin{aligned}\frac{F(N)}{F(M)} &= (-1)^{N-M} \prod_{\substack{M \leq j < N \\ p \nmid j}} j \\ &\equiv (-1)^{N-M}(-1)^k \pmod{p^n}.\end{aligned}$$

Here we have used Theorem 2.1 since there are k complete reduced residue systems in the product. Thus

$$\begin{aligned}\frac{F(N)}{F(M)} &\equiv (-1)^{k(p^n+1)} \pmod{p^n} \\ &\equiv 1^k \pmod{p^n} \\ &\equiv 1 \pmod{p^n},\end{aligned}$$

as required. □

Having established that Γ_p is well-defined, we turn to establishing its continuity. This is a consequence of the following result (the sequence definition of continuity).

Theorem 2.2. *Let $E \subseteq \mathbb{Z}_p$ and let $x_0 \in E$. For $f : E \to \mathbb{Q}_p$, f is continuous at*

$x_0 \in E$ if and only if for every sequence $\{x_n\} \in E$ satisfying $\lim_{n\to\infty} x_n = x_0$ we have

$$\lim_{n\to\infty} f(x_n) = f(x_0).$$

If we take $E = \mathbb{Z}_p$ then we see that Γ_p satisfies this property.

We observe that $\Gamma_p(N) = F(N)$ for nonnegative integers N. For positive integers n and N with $0 < N < p^n$, it follows from the definition of F and Theorem 2.1 that

$$F(N)F(p^n + 1 - N) \equiv (-1)^{E(N)} \pmod{p^n}, \tag{2.1}$$

where $E(N)$ is the least positive integer $\leq p$ congruent to $N \pmod{p}$. Taking a sequence of integers converging to $z \in \mathbb{Z}_p$ in (2.1) and using the continuity of $\Gamma_p(z)$ and $E(z)$, we obtain the reflection formula

$$\Gamma_p(z)\Gamma_p(1 - z) = (-1)^{E(z)}, \quad (z \in \mathbb{Z}_p). \tag{2.2}$$

Before Morita, in [31] Overholtzer gave a definition of a different p-adic analogue to the Γ-function (Overholtzer used $\Gamma_p(n) = \prod_{j=0}^{n-1}(1 + jp)$). This definition, however, does not prove as useful to our purposes as that of Morita.

2.3 Gauss and Jacobi Sums

Let p be prime and r a positive integer. We will set $q = p^r$ and denote the finite field with q elements by $\mathbb{F}_q$. To define Gauss and Jacobi sums over $\mathbb{F}_q$ we will first need the following definitions:

Definition 2.2. *A character of an abelian group G is a homomorphism $\chi : G \to \mathbb{C}^*$. In the case where $G = \mathbb{F}_q$ for some prime power q, characters of G are referred to as additive characters modulo q. In the case where $G = \mathbb{F}_q^*$, characters of G are referred to as multiplicative characters modulo q.*

From now on, when we refer simply to a "character", we shall mean a multiplicative character. Among such characters we have the *trivial character* that maps each element of $\mathbb{F}_q^*$ to 1, and we extend every multiplicative character to a map on $\mathbb{F}_q$ by agreeing that the trivial character is to map 0 to 1 while the other (nontrivial) characters are to map 0 to 0.

Definition 2.3. *With the above notation, we define the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ to be the group homomorphism* $\mathrm{tr} : \mathbb{F}_\mathrm{q} \to \mathbb{F}_\mathrm{p}$ *given by*

$$\mathrm{tr}(\alpha) := \sum_{\mathrm{j}=0}^{\mathrm{r}-1} \alpha^{\mathrm{p}^\mathrm{j}} \qquad (\alpha \in \mathbb{F}_\mathrm{q}).$$

We also denote by e the additive character $e : \mathbb{F}_q \to \mathbb{C}^*$ given by

$$e(\alpha) := e^{\frac{2\pi i \mathrm{tr}(\alpha)}{p}} \qquad (\alpha \in \mathbb{F}_q).$$

To see that $\mathrm{tr}(\alpha) \in \mathbb{F}_\mathrm{p}$ we use the multinomial theorem and the fact that $\mathbb{F}_q$ has characteristic p to obtain $(\alpha+\alpha^2+\ldots+\alpha^{p^{r-1}})^p = \alpha^p+\alpha^{p^2}+\ldots+\alpha^{p^r}$; but $\alpha^{p^r} = \alpha$, and so the equality becomes $(\mathrm{tr}(\alpha))^\mathrm{p} = \mathrm{tr}(\alpha)$, from which it follows that $\mathrm{tr}(\alpha) \in \mathbb{F}_\mathrm{p}$. To see that tr is a homomorphism we use the binomial theorem and the fact that $\mathbb{F}_q$ has characteristic p to obtain $\mathrm{tr}(\alpha+\beta) = \sum_{\mathrm{j}=0}^{\mathrm{r}-1}(\alpha+\beta)^{\mathrm{p}^\mathrm{j}} = \sum_{\mathrm{j}=0}^{\mathrm{r}-1}(\alpha^{\mathrm{p}^\mathrm{j}}+\beta^{\mathrm{p}^\mathrm{j}}) = \mathrm{tr}(\alpha)+\mathrm{tr}(\beta)$. The fact that e is an additive character follows from tr being a homomorphism.

We are now ready to define Gauss and Jacobi sums over the finite field $\mathbb{F}_q$.

Definition 2.4. *With the above notation, let χ be a character on $\mathbb{F}_q$, and $\beta \in \mathbb{F}_q$. Then the Gauss sum $G_r(\beta, \chi)$ over $\mathbb{F}_q$ is defined by*

$$G_r(\beta, \chi) = \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) e(\alpha\beta) = \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) e^{\frac{2\pi i \mathrm{tr}(\alpha\beta)}{p}}.$$

If $\beta = 1$, we shall write $G_r(1, \chi) = G_r(\chi)$. If $r = 1$, we shall suppress the subscript r.

Definition 2.5. *With the above notation, let χ and ψ be characters on $\mathbb{F}_q$. The Jacobi sum $J_r(\chi, \psi)$ is defined by*

$$J_r(\chi, \psi) = \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha)\psi(1-\alpha).$$

It is well known that the set of all characters of a finite abelian group G forms a group $\widehat{G}$, isomorphic to G and with the trivial character as its identity. In particular, the order of characters modulo q is well-defined and divides $\varphi(q)$. For two such characters, χ and ψ we define the *order* of the associated Jacobi sum to be the least common multiple of the orders of χ and ψ. In particular, if $J_r(\chi, \psi)$ has order m then the orders of χ and ψ both divide m. It follows that both χ and ψ map into the group of mth roots of unity so that $J_r(\chi, \psi)$ lies in the ring of integers of the cyclotomic field $\mathbb{Q}(e^{\frac{2\pi i}{m}})$, being a sum of mth roots of unity. For notational convenience, we suppress the subscript in the notation of the Jacobi sum when we are working modulo a prime. That is, we set $J(\chi, \psi) = J_1(\chi, \psi)$.

Lemma 2.2. *If χ is a nontrivial character on $\mathbb{F}_q$, then*

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = 0.$$

Proof. Since χ is nontrivial we know there exists $\beta \in \mathbb{F}_q^*$ such that $\chi(\beta) \neq 1$. Then

$$\begin{aligned} \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) &= \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha\beta) \quad \text{(since } \alpha \mapsto \alpha\beta \text{ defines a permutation of } \mathbb{F}_q^*\text{)} \\ &= \chi(\beta) \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha). \end{aligned}$$

Rearranging we get

$$(1 - \chi(\beta)) \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = 0.$$

Since $\chi(\beta) \neq 1$, we may conclude that

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = 0,$$

as required. □

An important relationship between Jacobi and Gauss sums is given by the following theorem. We present a proof to illustrate standard methods in dealing with these sums.

Theorem 2.3. *Let χ and ψ be characters on $\mathbb{F}_q$. If $\chi\psi$ is nontrivial, then*

$$J_r(\chi, \psi) = \frac{G_r(\chi)G_r(\psi)}{G_r(\chi\psi)}.$$

Proof. With χ and ψ as in the theorem, we have

$$\begin{aligned} G_r(\chi)G_r(\psi) &= \sum_{\alpha} \sum_{\beta} \chi(\alpha)\psi(\beta)e(\alpha)e(\beta) \\ &= \sum_{\alpha} \sum_{\beta} \chi(\alpha)\psi(\beta)e(\alpha+\beta) \\ &= \sum_{\gamma} e(\gamma) \sum_{\substack{\alpha,\beta \\ \alpha+\beta=\gamma}} \chi(\alpha)\psi(\beta) \\ &= \sum_{\substack{\alpha,\beta \\ \alpha+\beta=0}} \chi(\alpha)\psi(\beta) + \sum_{\gamma \neq 0} e(\gamma) \sum_{\alpha} \chi(\alpha)\psi(\gamma-\alpha). \end{aligned}$$

Thus

$$\begin{aligned} G_r(\chi)G_r(\psi) &= \psi(-1) \sum_{\alpha} \chi\psi(\alpha) + \sum_{\gamma \neq 0} e(\gamma) \sum_{\alpha} \chi(\alpha\gamma)\psi(\gamma - \alpha\gamma) \\ &= 0 + J_r(\chi, \psi) \sum_{\gamma \neq 0} \chi\psi(\gamma)e(\gamma) \quad \text{(by Lemma 2.2)} \\ &= J_r(\chi, \psi)G_r(\chi\psi). \end{aligned}$$

Here we have used the fact that $\chi\psi$ is nontrivial to conclude that $\chi\psi(0) = 0$ in the

last two equalities. This completes the proof. □

2.4 The Gross-Koblitz Formula

In the following chapter we will need to make use of a corollary of a special instance of the Gross-Koblitz formula. In its complete generality, the Gross-Koblitz formula is a powerful and celebrated result which expresses Gauss sums in terms of the value of Morita's p-adic Γ-function at rational arguments; see [21] and [1, Section 11.2].

Let $p = kf + 1$ be prime, g be a primitive root modulo p and χ be a character modulo p of order k such that $\chi(g) = \beta = e^{\frac{2\pi i}{k}}$.

We use the notation $L(a)$ to denote the least positive residue of the integer a modulo k. Write the base p expansion of $L(a)f$ as

$$L(a)f = a_0 + a_1 p + \ldots + a_{r-1}p^{r-1}, \qquad 0 \leq a_i \leq p-1,$$

and define $s(a)$ to be the sum of the base p digits of $L(a)f$:

$$s(a) = a_0 + a_1 + \ldots + a_{r-1}.$$

Set $\pi = e^{\frac{2\pi i}{p}} - 1$ and let λ be the prime element in $\mathbb{Q}_p(e^{\frac{2\pi i}{p}})$ such that

$$\lambda^{p-1} = -p \quad \text{and} \quad \lambda \equiv \pi \pmod{\pi^2}.$$

For the existence and uniqueness of λ, as well as additional information about $\mathbb{Q}_p(e^{\frac{2\pi i}{p}})$ see [23, Chapter 3].

A special instance of the Gross-Koblitz formula is then given by

$$G(\chi^{-a}) = -\lambda^{s(a)}\Gamma_p\left(\frac{L(a)}{k}\right) \quad \text{in } \mathbb{Q}_p(e^{\frac{2\pi i}{p}}),$$

where χ is the specific character defined above and Γ_p is Morita's p-adic gamma function ([1, Page 350]). For details regarding the Gross-Koblittz formula in all of its generality as well as commentary on its proof see [1, Sections 2.1 and 11.2].

We now use this formula together with Theorem 2.3 to express Jacobi sums in terms of the values of Morita's p-adic Γ-function at rational arguments.

Lemma 2.3. *Let χ be the character defined above and let a and b be positive integers such that $a + b \leq k$. Then*

$$J(\chi^{k-a}, \chi^{k-b}) = -\frac{\Gamma_p(\frac{a}{k})\Gamma_p(\frac{b}{k})}{\Gamma_p(\frac{a+b}{k})}.$$

Proof. With χ, k, a, and b as in statement of the lemma, we have

$$J(\chi, \psi) = \frac{G(\chi)G(\psi)}{G(\chi\psi)}$$

by Theorem 2.3 with $r = 1$. Replacing χ by χ^{k-a} and ψ by χ^{k-b} we get

$$\begin{aligned} J(\chi^{k-a}, \chi^{k-b}) &= \frac{G(\chi^{k-a})G(\chi^{k-b})}{G(\chi^{2k-(a+b)})} \\ &= \frac{(-\lambda^{s(a-k)}\Gamma_p(\frac{L(a-k)}{k})(-\lambda^{s(b-k)}\Gamma_p(\frac{L(b-k)}{k}))}{-\lambda^{s(-2k+(a+b))}\Gamma_p(\frac{L((a+b)-2k)}{k})}. \end{aligned}$$

Here we have applied the special instance of the Gross-Koblitz Formula three times. Then, using the definitions of $L(n)$ and $s(n)$, we get

$$\begin{aligned} J(\chi^{k-a}, \chi^{k-b}) &= -\frac{\lambda^{s(a-k)+s(b-k)}\Gamma_p(\frac{a}{k})\Gamma_p(\frac{b}{k})}{\lambda^{s(-2k+(a+b))}\Gamma_p(\frac{a+b}{k})} \\ &= -\frac{\Gamma_p(\frac{a}{k})\Gamma_p(\frac{b}{k})}{\Gamma_p(\frac{a+b}{k})}, \end{aligned}$$

as desired. □

By the reflection formula (2.2) and the identities

$$E\left(\frac{a}{k}\right) = p - af, \qquad E\left(\frac{b}{k}\right) = p - bf, \qquad E\left(\frac{a+b}{k}\right) = p - (a+b)f,$$

(valid for positive integers a, b with $a + b \leq k$) we get the following corollary:

Corollary 2.1. *For $\chi, k, a,$ and b as above we have*

$$J(\chi^{k-a}, \chi^{k-b}) = \frac{\Gamma_p(1 - \frac{a+b}{k})}{\Gamma_p(1 - \frac{a}{k})\Gamma_p(1 - \frac{b}{k})}.$$

2.5 Evaluations of Certain Jacobi Sums

Let $p = 4f+1$ be prime, g be a primitive root modulo p, and χ be a character modulo p of order 4 such that $\chi(g) = \beta$, where $\beta = \exp(\frac{2\pi i}{4}) = i$. Then the values of the 16 Jacobi sums $J(\chi^m, \chi^n)$ $(m, n = 0, 1, 2, 3)$ of order 4 are given in the table below.

$m \backslash n$	0	1	2	3
0	p	0	0	0
1	0	$(-1)^f(a_4 + ib_4)$	$a_4 + ib_4$	$-(-1)^f$
2	0	$a_4 + ib_4$	-1	$a_4 - ib_4$
3	0	$-(-1)^f$	$a_4 - ib_4$	$(-1)^f(a_4 - ib_4)$

Table 2.1: Table 3.2.1 in [1].

Let $p = 6f + 1$ be prime, g be a primitive root modulo p, and χ be a character modulo p of order 6 such that $\chi(g) = \beta$, where $\beta = \exp(\frac{2\pi i}{6}) = \frac{1+i\sqrt{3}}{2}$. Then the values of the 36 Jacobi sums $J(\chi^m, \chi^n)$ $(m, n = 0, 1, 2, 3, 4, 5)$ of order 6 are given in the table below.

$m\backslash^n$	0	1	2	3	4	5
0	p	0	0	0	0	0
1	0	$(-1)^f\frac{1}{2}(u_3+iv_3\sqrt{3})$	$a_3+ib_3\sqrt{3}$	$(-1)^f(a_3+ib_3\sqrt{3})$	$\frac{1}{2}(u_3+iv_3\sqrt{3})$	$-(-1)^f$
2	0	$a_3+ib_3\sqrt{3}$	$\frac{1}{2}(r_3+is_3\sqrt{3})$	$a_3+ib_3\sqrt{3}$	-1	$\frac{1}{2}(u_3-iv_3\sqrt{3})$
3	0	$(-1)^f\frac{1}{2}(a_3+ib_3\sqrt{3})$	$a_3+ib_3\sqrt{3}$	$-(-1)^f$	$a_3-ib_3\sqrt{3}$	$(-1)^f\frac{1}{2}(a_3-ib_3\sqrt{3})$
4	0	$\frac{1}{2}(u_3+iv_3\sqrt{3})$	-1	$a_3-ib_3\sqrt{3}$	$\frac{1}{2}(r_3-is_3\sqrt{3})$	$a_3-iv_3\sqrt{3}$
5	0	$-(-1)^f$	$\frac{1}{2}(u_3-iv_3\sqrt{3})$	$(-1)^f(a_3-ib_3\sqrt{3})$	$a_3-ib_3\sqrt{3}$	$(-1)^f\frac{1}{2}(u_3-iv_3\sqrt{3})$

Table 2.2: Table 3.1.2 in [1].

2.6 Some Special Number Sequences

In this section we give a few more details on the special numbers already mentioned in the Introduction.

Definition 2.6. *The Bernoulli polynomials $B_k(x), (k \geq 0)$ are defined by the exponential generating function*

$$\frac{te^{tx}}{e^t-1} = \sum_{k=0}^{\infty} \frac{B_k(x)}{k!}t^k,$$

and the Bernoulli numbers $B_0, B_1, B_2, \ldots$ by $B_k = B_k(0)$ $(k \geq 0)$.

Definition 2.7. *The Euler numbers E_k, $(k \geq 0)$ are defined by setting $E_{2k+1} = 0$ and*

$$E_{2k} = -4^{2k+1}\frac{B_{2k+1}(\frac{1}{4})}{2k+1} \quad (k \geq 0).$$

Taking $x = 0$ in the definition of the Bernoulli polynomial shows that the Bernoulli numbers are determined by the following exponential generating function:

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty} \frac{B_k}{k!}t^k.$$

Similarly, the Euler numbers are given by the following exponential generating function:

$$\frac{1}{\cosh(t)} = \frac{2}{e^t+e^{-t}} = \sum_{k=0}^{\infty} \frac{E_k}{k!}t^k.$$

The Bernoulli and Euler numbers and polynomials satisfy many recurrence relations as well as other important properties, as can be found in, e.g., [5] or [30, Chapter 24]. Bernoulli numbers and polynomials are by definition the Taylor coefficients of certain power series and therefore occur in the Taylor expansions of a number of classical functions. These numbers and polynomials have been studied in great detail and are found in many different areas of mathematics, including number theory, the analysis of finite differences, and numerical analysis. They have connections to certain Fourier series, analytic applications of L-functions, numerical integration, and Fermat's Last Theorem.

The following is a table containing the first few Bernoulli polynomials, Bernoulli numbers, and Euler numbers.

n	B_n	E_n	$B_n(x)$
0	1	1	1
1	$-1/2$	0	$x - \frac{1}{2}$
2	$1/6$	-1	$x^2 - x + \frac{1}{6}$
3	0	0	$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$
4	$-1/30$	5	$x^4 - 2x^3 + x^2 - \frac{1}{30}$
5	0	0	$x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x$
6	$1/42$	-61	$x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 + \frac{1}{42}$
7	0	0	$x^7 - \frac{7}{2}x^6 + \frac{7}{2}x^5 - \frac{7}{6}x^3 + \frac{1}{6}x$
8	$-1/30$	1385	$x^8 - 4x^7 + \frac{14}{3}x^6 - \frac{7}{3}x^4 + \frac{2}{3}x^2 - \frac{1}{30}$

Table 2.3: B_n, E_n, and $B_n(x)$ for $0 \leq n \leq 8$.

We will also make use of the following notation, defined in [32].

Definition 2.8. *The Fermat quotient of an integer a with respect to an odd prime $p \nmid a$ is defined by*

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

We note that this value will always be an integer by Fermat's Little Theorem. In particular, $2^{p-1} \equiv 1 \pmod{p}$ for odd primes p. Wieferich primes are those p for which we can do better. An odd prime p is called a *Wieferich prime* if $2^{p-1} \equiv 1 \pmod{p^2}$; this is equivalent to $q_p(2) \equiv 0 \pmod{p}$. It was shown in [16] that $p = 1093$ and $p = 3511$ are the only Wieferich primes with $p < 6.7 \times 10^{15}$. We also mention in passing that Wieferich primes have a connection to Fermat's Last Theorem, as for example can be found on [32, Page 23].

2.7 Congruences for Certain Finite Sums

In order to prove some of our results we need a number of congruences for certain finite sums. Congruences of this kind were obtained by several authors in the early 1900s; here we will focus on results that are found in the papers [24] of Emma Lehmer and [33] of Zhi-Hong Sun.

Lemma 2.4. *For all primes $p \geq 5$ we have*

$$\sum_{j=1}^{p-1} \frac{1}{j^2} \equiv 0 \pmod{p}, \tag{2.3}$$

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j^2} \equiv 0 \pmod{p}, \tag{2.4}$$

$$\sum_{1 \leq j < k \leq p-1} \frac{1}{jk} \equiv 0 \pmod{p}, \tag{2.5}$$

$$\sum_{1 \leq j < k \leq \frac{p-1}{2}} \frac{1}{jk} \equiv 2q_p(2)^2 \pmod{p}, \tag{2.6}$$

for $p \equiv 1 \pmod{4}$, we have

$$\sum_{j=1}^{\frac{p-1}{4}} \frac{1}{j^2} \equiv 4E_{p-3} \pmod{p}, \tag{2.7}$$

$$\sum_{1 \leq j < k \leq \frac{p-1}{4}} \frac{1}{jk} \equiv \frac{9}{2} q_p(2)^2 - 2E_{p-3} \pmod{p}, \tag{2.8}$$

and for $p \equiv 1 \pmod 3$, *we have*

$$\sum_{j=1}^{\frac{2(p-1)}{3}} \frac{1}{j^2} \equiv -\frac{1}{2} B_{p-2}\left(\tfrac{1}{3}\right) \pmod p, \tag{2.9}$$

$$\sum_{j=1}^{\frac{p-1}{3}} \frac{1}{j^2} \equiv \frac{1}{2} B_{p-2}\left(\tfrac{1}{3}\right) \pmod p, \tag{2.10}$$

$$\sum_{1 \le j < k \le \frac{2(p-1)}{3}} \frac{1}{jk} \equiv \frac{9}{8} q_p(3)^2 + \frac{1}{4} B_{p-2}\left(\tfrac{1}{3}\right) \pmod p, \tag{2.11}$$

$$\sum_{1 \le j < k \le \frac{p-1}{3}} \frac{1}{jk} \equiv \frac{9}{8} q_p(3)^2 - \frac{1}{4} B_{p-2}\left(\tfrac{1}{3}\right) \pmod p. \tag{2.12}$$

Lemma 2.5. *For all primes* $p \ge 5$ *we have*

$$\sum_{j=1}^{p-1} \frac{1}{j} \equiv 0 \pmod{p^2}, \tag{2.13}$$

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j} \equiv -2q_p(2) + pq_p(2)^2 \pmod{p^2}, \tag{2.14}$$

for $p \equiv 1 \pmod 4$, *we have*

$$\sum_{j=1}^{\frac{p-1}{4}} \frac{1}{j} \equiv -3q_p(2) + \frac{3}{2} pq_p(2)^2 - pE_{p-3} \pmod{p^2}, \tag{2.15}$$

and for $p \equiv 1 \pmod 3$ *we have*

$$\sum_{j=1}^{\frac{2(p-1)}{3}} \frac{1}{j} \equiv -\frac{3}{2} q_p(3) + \frac{3}{4} pq_p(3)^2 + \frac{1}{3} B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p^2}, \tag{2.16}$$

$$\sum_{j=1}^{\frac{p-1}{3}} \frac{1}{j} \equiv -\frac{3}{2} q_p(3) + \frac{3}{4} pq_p(3)^2 - \frac{1}{6} B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p^2}. \tag{2.17}$$

For odd primes p and integers $a \not\equiv 0 \pmod p$, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if $x^2 \equiv a \pmod p$ has a solution and -1 otherwise. In general, the values of

$\left(\frac{a}{p}\right)$ are determined by the residue class of p modulo $4|a|$. Of particular interest to us will be the $a = 2$ and $a = 3$ cases given by the following two lemmas.

Lemma 2.6.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Lemma 2.7.

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

We are now ready to state the next set of summation congruences.

Lemma 2.8. *For all primes $p \geq 7$ we have*

$$\sum_{j=1}^{\lfloor \frac{p-1}{6} \rfloor} \frac{1}{j^2} \equiv \frac{1}{2}\left(\frac{p}{3}\right) B_{p-2}\left(\tfrac{1}{6}\right) \pmod p, \tag{2.18}$$

$$\begin{aligned} \sum_{j=1}^{\lfloor \frac{p-1}{6} \rfloor} \frac{1}{j} \equiv & -2q_p(2) - \frac{3}{2}q_p(3) + p\left(q_p(2)^2 + \frac{3}{4}q_p(3)^2\right) \\ & - \frac{p}{12}\left(\frac{p}{3}\right) B_{p-2}\left(\tfrac{1}{6}\right) \pmod{p^2}. \end{aligned} \tag{2.19}$$

In order to find modulo p^3 identities for some Gauss factorials, we require sums that are very similar to the ones above. These sums were not found in the literature directly; however, they are easy to obtain from the results in [24] and [33], as was done in [7].

In [24] we find the congruence

$$\frac{1}{nr} \equiv \frac{-1}{p - nr} - p\frac{1}{n^2r^2} \pmod{p^2},$$

valid for primes p and integers n, r such that $p \nmid n, r$.

If we take $n = 1$ and $r = j$, we obtain

$$\frac{1}{j} \equiv \frac{-1}{p-j} - p\frac{1}{j^2} \pmod{p^2}. \tag{2.20}$$

Thus, for $p \equiv 1 \pmod 4$,

$$\sum_{j=1}^{\frac{3(p-1)}{4}} \frac{1}{j} = \sum_{j=1}^{p-1} \frac{1}{j} - \sum_{j=1}^{\frac{p-1}{4}} \frac{1}{p-j}, \equiv -\sum_{j=1}^{\frac{p-1}{4}} \frac{1}{p-j} \pmod{p^2}, \text{ by (2.13)}.$$

Using (2.20), we then obtain

$$\sum_{j=1}^{\frac{3(p-1)}{4}} \frac{1}{j} \equiv \sum_{j=1}^{\frac{p-1}{4}} \frac{1}{j} + p\sum_{j=1}^{\frac{p-1}{4}} \frac{1}{j^2} \pmod{p^2}. \tag{2.21}$$

Finally we invoke Lemmas 2.4 and 2.5 to obtain the following lemma.

Lemma 2.9. *For all primes $p \equiv 1 \pmod 4$, we have*

$$\sum_{j=1}^{\frac{3(p-1)}{4}} \frac{1}{j} \equiv -3q_p(2) + \frac{3}{2}pq_p(2)^2 + 3pE_{p-3} \pmod{p^2}.$$

To obtain an analogous result for the other type of sum considered in the above lemmas (still considering $p \equiv_4 1$), we start with the observation that

$$\sum_{1 \le j < k \le \frac{3(p-1)}{4}} \frac{1}{jk} = \frac{1}{2}\left(\sum_{j=1}^{\frac{3(p-1)}{4}} \frac{1}{j}\right)^2 - \frac{1}{2}\sum_{j=1}^{\frac{3(p-1)}{4}} \frac{1}{j^2}. \tag{2.22}$$

However, from our work above we see that

$$\begin{aligned}\sum_{j=1}^{\frac{3(p-1)}{4}} \frac{1}{j^2} &= \sum_{j=1}^{p-1} \frac{1}{j^2} - \sum_{j=1}^{\frac{p-1}{4}} \frac{1}{(p-j)^2} \\ &\equiv -\sum_{j=1}^{\frac{p-1}{4}} \frac{1}{j^2} \equiv -4E_{p-3} \pmod{p},\end{aligned} \tag{2.23}$$

where we have used (2.3) and (2.7). We conclude that

$$\begin{aligned}\sum_{1\le j<k\le\frac{3(p-1)}{4}}\frac{1}{jk} &= \frac{1}{2}\left(\sum_{j=1}^{\frac{3(p-1)}{4}}\frac{1}{j}\right)^2-\frac{1}{2}\sum_{j=1}^{\frac{3(p-1)}{4}}\frac{1}{j^2} \quad \text{(from (2.22))}\\ &\equiv \frac{1}{2}\left(\sum_{j=1}^{\frac{3(p-1)}{4}}\frac{1}{j}\right)^2-\frac{1}{2}(-4E_{p-3}) \pmod p \quad \text{(from (2.23))}\\ &\equiv \frac{1}{2}(-3q_p(2))^2+2E_{p-3} \pmod p \quad \text{(from Lemma 2.9)}\\ &= \frac{9}{2}q_p(2)^2+2E_{p-3}.\end{aligned}$$

We have therefore proved the following congruence:

Lemma 2.10. *For all primes $p\equiv 1 \pmod 4$, we have*

$$\sum_{1\le j<k\le\frac{3(p-1)}{4}}\frac{1}{jk}\equiv\frac{9}{2}q_p(2)^2+2E_{p-3} \pmod p.$$

In a completely analogous manner we get the following useful congruences:

Lemma 2.11. *For all primes $p\equiv 1 \pmod 6$, we have*

$$\sum_{j=1}^{\frac{5(p-1)}{6}}\frac{1}{j}\equiv -2q_p(2)-\frac{3}{2}q_p(3)+pq_p(2)^2+\frac{3}{4}pq_p(3)^2+\frac{25}{12}pB_{p-2}\left(\tfrac{1}{3}\right) \pmod{p^2},$$

$$\sum_{1\le j<k\le\frac{5(p-1)}{6}}\frac{1}{jk}\equiv 2q_p(2)^2+3q_p(2)q_p(3)+\frac{9}{8}q_p(3)^2+\frac{5}{4}B_{p-2}\left(\tfrac{1}{3}\right) \pmod p.$$

Employing the same method used in (2.22), we have

$$\sum_{1\le j<k\le\lfloor\frac{p}{6}\rfloor}\frac{1}{jk}=\frac{1}{2}\left(\sum_{j=1}^{\lfloor\frac{p}{6}\rfloor}\frac{1}{j}\right)^2-\frac{1}{2}\sum_{j=1}^{\lfloor\frac{p}{6}\rfloor}\frac{1}{j^2},$$

and ultimately obtain the following analogue to Lemma 2.10.

Lemma 2.12. *For all primes $p \equiv 1 \pmod 6$, we have*

$$\sum_{1 \le j < k \le \frac{p-1}{6}} \frac{1}{jk} \equiv 2q_p(2)^2 + 3q_p(2)q_p(3) + \frac{9}{8}q_p(3)^2 - \frac{1}{4}\left(\frac{3}{p}\right) B_{p-2}\left(\tfrac{1}{6}\right) \pmod p.$$

2.8 Primes and Sums of Squares

The following section very closely follows [12, Chapter 1]. A famous theorem in elementary number theory, conjectured by Fermat and then proved by Euler, is the following:

Theorem 2.4. *An odd prime p can be written as a sum of two integer squares if and only if $p \equiv 1 \pmod 4$.*

For the sake of completeness, we present a proof, based on the exposition in [12, pp. 10–12].

Proof of Theorem 2.4. First assume $p = x^2 + y^2$ for suitable integers x and y. The squares modulo 4 are 0 and 1 which means that p must be congruent to one of 0,1,2 modulo 4. However since p is odd, it cannot be congruent to 0 or 2 modulo 4 and we must have $p \equiv 1 \pmod 4$, as required.

Conversely, assume $p \equiv 1 \pmod 4$. We show that $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$ using the method of infinite descent:

Claim (Descent Step)**.** *If an odd prime divides a sum of two relatively prime squares then it is itself a sum of two squares.*

Proof of Descent Step. To prove this step, we will require the following lemma.

Lemma 2.13. *Suppose that N is a sum of two relatively prime squares, and that $q = x^2 + y^2$ is a prime divisor of N. Then $\frac{N}{q}$ is also a sum of two relatively prime squares.*

Proof of lemma. Write $N = a^2 + b^2$, where a and b are relatively prime, and suppose that $q = x^2 + y^2$ is a prime divisor of N. Then q also divides

$$\begin{aligned} x^2N - a^2q &= x^2(a^2 + b^2) - a^2(x^2 + y^2) \\ &= x^2b^2 - a^2y^2 \\ &= (xb - ay)(xb + ay). \end{aligned}$$

Since q is prime, it divides one of these two factors, and changing the sign of a, if necessary, we can assume that $q \mid (xb - ay)$. Thus $xb - ay = dq$ for some integer d. We claim that $x \mid (a + dy)$. Since x and y are relatively prime, this is equivalent to $x \mid (a + dy)y$. However,

$$\begin{aligned} (a + dy)y &= ay + dy^2 \\ &= xb - dq + dy^2 \\ &= xb - d(x^2 + y^2) + dy^2 \\ &= xb - dx^2, \end{aligned}$$

which is divisible by x. Furthermore, if we set $a + dy = cx$ for a suitable integer c, then the last equality implies that $b = dx + cy$. Thus

$$a = cx - dy \tag{2.24}$$

$$b = dx + cy. \tag{2.25}$$

Then, using (2.24) and (2.25), we obtain

$$\begin{aligned} N &= a^2 + b^2 \\ &= (cx - dy)^2 + (dx + cy)^2 \\ &= (x^2 + y^2)(c^2 + d^2) \\ &= q(c^2 + d^2). \end{aligned}$$

Thus $\frac{N}{q} = c^2 + d^2$ is a sum of two squares, and (2.24) and (2.25) show that c and d must be relatively prime since a and b are. We have now completed the proof of our lemma.

We now return to the proof of the descent step.

Suppose, towards a contradiction, that p is an odd prime dividing $N = a^2 + b^2$, where a and b are relatively prime and p is not the sum of two squares. If a and b are changed by adding multiples of p, we still have $p \mid a^2 + b^2$. We may therefore assume that $|a| < \frac{p}{2}$ and $|b| < \frac{p}{2}$, which in turn implies that $N < \frac{p^2}{2}$. The new a and b may have a greatest common divisor $d > 1$, but p does not divide d, so that by dividing a and b by d, if necessary, we may assume that $p \mid N$, $N < \frac{p^2}{2}$, and $N = a^2 + b^2$ where $\gcd(a, b) = 1$. Then all prime divisors $q \neq p$ of N are less than p. If q were a sum of two squares, then Lemma 2.13 would show that $\frac{N}{q}$ would be a multiple of p, which is also a sum of two squares. If all such q's were sums of two squares, then repeatedly applying Lemma 2.13 would imply that p itself was of the same form. So if p is not a sum of two squares, there must be a smaller prime q with the desired property. Since there is nothing to prevent us from repeating this process indefinitely, we can create an infinite decreasing sequence of prime numbers. This contradiction finishes the Descent Step.

Claim (Reciprocity Step)**.** *If $p \equiv 1 \pmod 4$ then p divides a sum of two relatively prime squares.*

Proof of Reciprocity Step. Since $p \equiv 1 \pmod 4$, we can write $p = 4k+1$ for a suitable integer k. Then Fermat's Little Theorem implies that

$$(x^{2k} - 1)(x^{2k} + 1) = x^{4k} - 1 \equiv 0 \pmod p$$

for all $x \not\equiv 0 \pmod p$. If $x^{2k} - 1 \not\equiv 0 \pmod p$ for one such x, then $p \mid x^{2k} + 1$, so that p divides a sum of relatively prime squares, as desired. The required x is guaranteed to exist by the fundamental theorem of algebra, since $x^{2k} - 1$ is a polynomial over

the field $\mathbb{F}_p$ and hence has at most $2k < p-1$ roots. This completes the proof of the Reciprocity Step which in turn completes the proof of Theorem 2.4. □

This is only the first of many related results that are due to Fermat. For example, the following were also stated by Fermat and then proved by Euler:

Theorem 2.5. *An odd prime p can be written as $p = x^2 + 2y^2$ where $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 3 \pmod 8$.*

Theorem 2.6. *An odd prime p can be written as $p = x^2 + 3y^2$ where $x, y \in \mathbb{Z}$ if and only if $p \not\equiv 2 \pmod 3$.*

These two theorems can be proven analogously to the above theorem if we change the Descent Steps respectively to:

Claim. *If an odd prime divides a sum of a square and two times another relatively prime square then it is itself of the same form.*

Claim. *If an odd prime divides a sum of a square and three times another relatively prime square then it is itself of the same form.*

and change the Reciprocity Steps respectively to:

Claim. *If $p \equiv 1, 3 \pmod 8$ then p divides a sum of a square and two times another relatively prime square.*

Claim. *If $p \equiv 1 \pmod 3$ then p divides a sum of a square and three times another relatively prime square.*

We note that when we write $p = x^2 + y^2$, $p = x^2 + 2y^2$, or $p = x^2 + 3y^2$ for integers x and y, these representations are unique up to the sign of x and y. For proofs of this, see [29, pp. 167–174], in particular, Corollary 3.23 and Theorem 3.27 with $d = -12$ and $d = -8$, respectively.

When considering the general case given by $p = x^2 + ny^2$ for integers x and y and an arbitrary positive integer n, Euler's two-step method above will not lead to a proof. Indeed, the fact that a prime divides an integer of this form need not imply that the prime is of the same form. For example, consider $n = 5$: $3 \mid 21 = 1^2 + 5 \cdot 2^2$ but $3 \neq x^2 + 5y^2$ for integers x and y.

To completely answer the question of when a prime can be written as $p = x^2 + ny^2$ for integers x, y, and a given positive integer n, we would need to employ methods that lie beyond the scope of this thesis. We refer the interested reader to [12] for a complete discussion of the subject.

Chapter 3

Congruences for Binomial Coefficients Modulo p^3

The goal of this chapter is to derive modulo p^3 analogues for as many classes of binomial coefficients as possible. Using [7] as a guide, in each case we will do this in two stages: First we will derive congruences modulo arbitrarily high powers of p for quotients of suitable Gauss factorials. These results will then be used to prove the desired modulo p^3 congruences for binomial coefficients. Due to the nature of the proofs, there will be a great deal of repetition throughout this chapter.

3.1 The $p \equiv 1 \pmod 6$ case

Let $p = 6f + 1$ be a prime and let g be a primitive root modulo p. Define $Z = \mathrm{ind}_g 2$, $\beta = \exp(\frac{2\pi i}{6}) = \frac{1+i\sqrt{3}}{2}$ a primitive 6th root of unity, and χ a character modulo p of order 6 such that $\chi(g) = \beta$. By Theorem 2.6 and the argument presented in Chapter 1, we can write

$$p = a_3^2 + 3b_3^2, \quad a_3 \equiv -1 \pmod 3, \quad b_3 \equiv -Z \pmod 3. \tag{3.1}$$

It follows that, with $u_3 = 2a_3^2, v_3 = 2b_3^2$,

$$4p = u_3^2 + 3v_3^2, \quad u_3 \equiv 1 \pmod 3, \quad v_3 \equiv Z \pmod 3. \tag{3.2}$$

We will obtain several modulo p and modulo p^2 congruences in this section. The modulo p^2 ones can be obtained from [1, Theorem 9.4.4], and the modulo p ones can either be deduced from their modulo p^2 analogues, or can be found directly in [1, Theorem 9.2.5].

3.1.1 The binomial coefficient $\binom{\frac{p-1}{3}}{\frac{p-1}{6}}$

In [1] we find the following two congruences:

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1}u_3 \equiv \begin{cases} 2(-1)^{\frac{p-1}{6}+1}a_3 & \pmod p \text{ if } b_3 \equiv 0 \pmod 3, \\ (-1)^{\frac{p-1}{6}}(a_3+3b_3) & \pmod p \text{ if } b_3 \equiv 1 \pmod 3, \\ (-1)^{\frac{p-1}{6}}(a_3-3b_3) & \pmod p \text{ if } b_3 \equiv 2 \pmod 3. \end{cases}$$

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1}\left(u_3 - \frac{p}{u_3}\right)\left(1+\frac{2^p-2}{3}\right) \pmod{p^2}.$$

The modulo p congruence is in fact due to Hudson and Williams [22]. We will begin by giving an independent proof of the theorem of Cosgrave and Dilcher (Theorem 1.10), which provides the following generalization:

$$\frac{(\frac{p^\alpha-1}{3})_p!}{((\frac{p^\alpha-1}{6})_p!)^2} \equiv (-1)^{\frac{p-1}{6}+1}\left(u_3 + u_3\sum_{j=1}^{\alpha-1}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{u_3^2}\right)^j\right) \pmod{p^\alpha}.$$

From [1, Table 3.1.2] we have

$$J(\chi,\chi) = (-1)^{\frac{p-1}{6}}\frac{1}{2}\left(u_3 + iv_3\sqrt{3}\right),$$

$$J(\chi^5,\chi^5) = (-1)^{\frac{p-1}{6}}\frac{1}{2}\left(u_3 - iv_3\sqrt{3}\right).$$

Furthermore, if $\mathfrak{p}$ is a nonzero prime ideal in the ring $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ of integers of $\mathbb{Q}(i\sqrt{3})$ dividing the prime p, then by [1, Theorem 2.1.14], we have

$$J(\chi,\chi) \equiv 0 \pmod{\mathfrak{p}}. \tag{3.3}$$

By taking $a = b = 1$ in Corollary 2.1, we obtain

$$J(\chi^5,\chi^5) = \frac{\Gamma_p(1-\frac{1}{3})}{\Gamma_p(1-\frac{1}{6})^2}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^5, \chi^5) \equiv \frac{\Gamma_p(1 + \frac{p^\alpha - 1}{3})}{\Gamma_p(1 + \frac{p^\alpha - 1}{6})^2} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^5, \chi^5) \equiv \frac{F(1 + \frac{p^\alpha - 1}{3})}{F(1 + \frac{p^\alpha - 1}{6})^2} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^5, \chi^5) \equiv -\frac{(\frac{p^\alpha - 1}{3})_p!}{((\frac{p^\alpha - 1}{6})_p!)^2} \pmod{p^\alpha}.$$

Here we have used the fact that $1 + \frac{p^\alpha - 1}{3} \equiv 1 \pmod 2$ which takes care of the minus sign. Next, (3.3) implies that $J(\chi, \chi)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}$. Thus

$$\left((-1)^{\frac{p-1}{6}} \frac{1}{2}(u_3 + iv_3\sqrt{3})\right)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

Since this holds for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ dividing p, we may conclude that this congruence also holds modulo p^α. Indeed, we know that p either remains prime in $\mathbb{Q}(i\sqrt{3})$, splits in $\mathbb{Q}(i\sqrt{3})$, or ramifies in $\mathbb{Q}(i\sqrt{3})$. In the first case,

$$\left((-1)^{\frac{p-1}{6}} \frac{1}{2}(u_3 + iv_3\sqrt{3})\right)^\alpha \in p^\alpha \mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$$

and in the other two cases,

$$\left((-1)^{\frac{p-1}{6}} \frac{1}{2}(u_3 + iv_3\sqrt{3})\right)^{2\alpha} \in p^\alpha \mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right].$$

We now have that

$$(u_3 + iv_3\sqrt{3})^\alpha \equiv 0 \pmod{p^\alpha}.$$

Expanding the left-hand side using the binomial theorem, we get

$$\sum_{j=0}^{\alpha} \binom{\alpha}{j} u_3^{\alpha-j} (iv_3\sqrt{3})^j \equiv 0 \pmod{p^\alpha}.$$

We separate the even from the odd powers to get

$$\sum_{j=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha}{2j} (-1)^j u_3^{\alpha-2j} 3^j v_3^{2j} + \sum_{j=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha}{2j+1} (-1)^j u_3^{\alpha-2j-1} 3^j v_3^{2j} (iv_3\sqrt{3}) \equiv 0 \pmod{p^\alpha}.$$

Grouping the real terms to one side of the congruence and the imaginary terms to the other side we have

$$-iv_3\sqrt{3} \sum_{j=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha}{2j+1} (-1)^j u_3^{\alpha-2j-1} 3^j v_3^{2j} \equiv \sum_{j=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha}{2j} (-1)^j u_3^{\alpha-2j} 3^j v_3^{2j} \pmod{p^\alpha}.$$

Because of the relationship $3v_3^2 = 4p - u_3^2$, the first sum, which we denote by S_1, becomes

$$\begin{aligned}
S_1 &= \sum_{j=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha}{2j+1} (-1)^j u_3^{\alpha-2j-1} (4p - u_3^2)^j \\
&= \sum_{j=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha}{2j+1} (-1)^j u_3^{\alpha-2j-1} \sum_{k=0}^{j} \binom{j}{k} (4p)^{j-k} (-u_3^2)^k \\
&= \sum_{j=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \sum_{k=0}^{j} \binom{\alpha}{2j+1} \binom{j}{k} (-1)^{j+k} u_3^{\alpha-1-2j+2k} (4p)^{j-k} \\
&= u_3^{\alpha-1} \sum_{j=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \sum_{k=0}^{j} \binom{\alpha}{2j+1} \binom{j}{k} \left(\frac{-4p}{u_3^2}\right)^{j-k}.
\end{aligned}$$

Setting $\nu = j - k$ and noting that $\binom{j}{k} = \binom{j}{j-k} = \binom{j}{\nu}$, we get

$$S_1 = u_3^{\alpha-1} \sum_{\nu=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \left(\frac{-4p}{u_3^2}\right)^{\nu} \sum_{j=\nu}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha}{2j+1} \binom{j}{\nu}.$$

We now use [18, Identity (3.1.21)], namely

$$\sum_{k=j}^{\lfloor \frac{n}{2} \rfloor} \binom{n+1}{2k+1} \binom{k}{j} = 2^{n-2j} \binom{n-j}{j}.$$

With this we obtain

$$S_1 = (2u_3)^{\alpha-1} \sum_{\nu=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha-1-\nu}{\nu} \left(\frac{-p}{u_3^2}\right)^{\nu}.$$

Similarly, the second sum, denoted by S_2, becomes

$$\begin{aligned}
S_2 =& \sum_{j=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha}{2j} (-1)^j u_3^{\alpha-2j} (4p - u_3^2)^j \\
=& \sum_{j=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha}{2j} (-1)^j u_3^{\alpha-2j} \sum_{k=0}^{j} \binom{j}{k} (4p)^{j-k} (-u_3^2)^k \\
=& \sum_{j=0}^{\lfloor \frac{\alpha}{2} \rfloor} \sum_{k=0}^{j} \binom{\alpha}{2j} \binom{j}{k} (-1)^{j+k} u_3^{\alpha-2j+2k} (4p)^{j-k} \\
=& u_3^{\alpha} \sum_{j=0}^{\lfloor \frac{\alpha}{2} \rfloor} \sum_{k=0}^{j} \binom{\alpha}{2j} \binom{j}{k} \left(\frac{-4p}{u_3^2}\right)^{j-k} \\
=& u_3^{\alpha} \sum_{\nu=0}^{\lfloor \frac{\alpha}{2} \rfloor} \left(\frac{-4p}{u_3^2}\right)^{\nu} \sum_{j=\nu}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha}{2j} \binom{j}{\nu}.
\end{aligned}$$

Using [18, Identity (3.120)], namely

$$\sum_{k=j}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} \binom{k}{j} = 2^{n-2j-1} \binom{n-j}{j} \frac{n}{n-j},$$

we obtain

$$S_2 = \frac{1}{2} (2u_3)^{\alpha} \sum_{\nu=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha-\nu}{\nu} \frac{\alpha}{\alpha-\nu} \left(\frac{-p}{u_3^2}\right)^{\nu}.$$

To simplify notation, we set $y = \frac{-p}{u_3^2}$. Now $S_1 \not\equiv 0 \pmod{p^{\alpha}}$; we can therefore divide by S_1 to obtain $-iv_3\sqrt{3} \equiv \frac{S_2}{S_1} \pmod{p^{\alpha}}$.

Claim. *We also have*

$$\frac{S_2}{S_1} \equiv u_3 + 2u_3 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} y^j \pmod{p^\alpha}.$$

Proof of Claim. This is equivalent to

$$\frac{\sum_{\nu=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha-\nu}{\nu} \frac{\alpha}{\alpha-\nu} y^\nu}{\sum_{\nu=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha-1-\nu}{\nu} y^\nu} \equiv 1 + 2 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} y^j \pmod{p^\alpha},$$

or

$$\begin{aligned}
&\sum_{\nu=0}^{\lfloor \frac{\alpha}{2} \rfloor} \left[\binom{\alpha-\nu}{\nu} \frac{\alpha}{\alpha-\nu} - \binom{\alpha-1-\nu}{\nu} \right] y^\nu \\
&\quad \equiv 2 \left(\sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} y^j \right) \left(\sum_{\nu=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha-1-\nu}{\nu} y^\nu \right) \\
&\quad \equiv 2 \sum_{j=1}^{\alpha-1} \sum_{\nu=0}^{\lfloor \frac{\alpha}{2} \rfloor} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \binom{\alpha-1-\nu}{\nu} y^{j+\nu} \pmod{p^\alpha}.
\end{aligned}$$

We can simplify the left-hand side of the congruence by using the identity $\binom{\alpha-\nu}{\nu} \frac{\alpha}{\alpha-\nu} - \binom{\alpha-1-\nu}{\nu} = 2\binom{\alpha-1-\nu}{\nu-1}$, which follows readily from the definition of the binomial coefficient. To simplify the right-hand side, we will set $k = j + \nu$ and change the order of summation. When we do this, we get

$$\sum_{\nu=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha-1-\nu}{\nu-1} y^\nu \equiv \sum_{k=1}^{\alpha-1} \left(\sum_{j=1}^{k} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \binom{\alpha-1+j-k}{k-j} \right) y^k \pmod{p^\alpha}.$$

We have proven our claim if we can show that the coefficients of the powers of y on both sides of our last congruence are equal up to the power $\alpha - 1$. To see that this is indeed the case, we use the identity

$$\sum_{j \geq 0} \frac{(-1)^j}{j+1} \binom{2j}{j} \binom{n+j}{n-m-j} = \binom{n-1}{n-m},$$

which can be obtained from [19, Identity (3.120)] by setting $n = \alpha - k$ and $n - m = k - 1$.

We have now proved Theorem 1.10, which we state again for the sake of completeness.

Theorem 3.1. *With p and u_3 as described in* (3.1)–(3.2)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(\frac{p^\alpha-1}{3})_p!}{((\frac{p^\alpha-1}{6})_p!)^2} \equiv (-1)^{\frac{p-1}{6}+1}\left(u_3 + u_3\sum_{j=1}^{\alpha-1}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{u_3^2}\right)^j\right) \pmod{p^\alpha}.$$

To obtain our analogue to Theorem 1.3, we have to translate the congruence in Theorem 3.1 into a congruence involving binomial coefficients. The quotient of Gauss factorials on the left-hand side is very similar to a central binomial coefficient. We begin by noting that for primes p as above and positive integers d with $d \nmid (p-1)$, we have

$$\frac{p^3-1}{d} = \frac{p^2-1}{d}p + \frac{p-1}{d}.$$

Thus, with $s = \frac{p^2-1}{d}$ we have

$$\left(\frac{p^3-1}{d}\right)_p! = \prod_{\nu=0}^{s-1}[(\nu p+1)\dots(\nu p+p-1)]\left[(sp+1)\dots\left(sp+\frac{p-1}{d}\right)\right].$$

Now for each $\nu = 0, 1, \dots, s-1$ we have

$$(\nu p+1)\dots(\nu p+p-1) = (p-1)!\left[1+\nu p\sum_{j=1}^{p-1}\frac{1}{j} + \nu^2p^2\sum_{1\le j<k\le p-1}\frac{1}{jk}\right]$$

$$\equiv (p-1)! \pmod{p^3}.$$

Here we have used Lemmas 2.4 and 2.5. Similarly,

$$(sp+1)\dots(sp+\tfrac{p-1}{d}) \equiv \left(\frac{p-1}{d}\right)!\left[1+sp\sum_{j=1}^{\frac{p-1}{d}}\frac{1}{j} + s^2p^2\sum_{1\le j<k\le\frac{p-1}{d}}\frac{1}{jk}\right] \pmod{p^3}.$$

When $d = 3$ we obtain

$$(sp+1)\dots(sp+\tfrac{p-1}{3}) \equiv \left(\frac{p-1}{3}\right)!\left[1+sp\left(\frac{-3}{2}q_p(3)+\frac{3}{4}pq_p(3)^2-\frac{1}{6}pB_{p-2}\left(\tfrac{1}{3}\right)\right)\right.$$
$$\left.+s^2p^2\left(\frac{9}{8}q_p(3)^2-\frac{1}{4}B_{p-2}\left(\tfrac{1}{3}\right)\right)\right] \pmod{p^3}.$$

Here we have used Lemmas 2.4 and 2.5. Upon simplifying and using the fact that $s \equiv -\frac{1}{3} \pmod{p^2}$, we obtain

$$\left(\frac{p^3-1}{3}\right)_p ! \equiv (p-1)!^{\frac{p^2-1}{3}}\left(\frac{p-1}{3}\right)!$$
$$\times\left(1+\frac{1}{2}pq_p(3)-\frac{1}{8}p^2q_p(3)^2+\frac{1}{36}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.$$

When $d = 6$, we will have to make use of Lemma 2.12. Proceeding as we did before, we get

$$\left(\frac{p^3-1}{6}\right)_p ! \equiv (p-1)!^{\frac{p^2-1}{6}}\left(\frac{p-1}{6}\right)!\left(1+sp\sum_{j=1}^{\frac{p-1}{6}}\frac{1}{j}+s^2p^2\sum_{1\le j<k\le\frac{p-1}{6}}\frac{1}{jk}\right) \pmod{p^3}.$$

Now $s \equiv \frac{-1}{6} \pmod{p^2}$, and so, upon simplifying, we get

$$\left(\frac{p^3-1}{6}\right)_p ! \equiv (p-1)!^{\frac{p^2-1}{6}}\left(\frac{p-1}{6}\right)!\left(1+\frac{1}{3}pq_p(2)+\frac{1}{4}pq_p(3)-\frac{1}{9}p^2q_p(2)^2\right.$$
$$\left.-\frac{3}{32}p^2q_p(3)^2+\frac{1}{12}p^2q_p(2)q_p(3)+\frac{1}{144}p^2\left(\frac{3}{p}\right)B_{p-2}\left(\tfrac{1}{6}\right)\right) \pmod{p^3}.$$

Combining everything, we get the desired analogue to Theorem 1.3:

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1}\left(u_3-\frac{p}{u_3}-\frac{p^2}{u_3^3}\right)$$
$$\times\frac{A}{\left(1+\frac{1}{2}pq_p(3)-\frac{1}{8}p^2q_p(3)^2+\frac{1}{36}p^2B_{p-2}(\frac{1}{3})\right)} \pmod{p^3},$$

where

$$A = \left(1 + \frac{2}{3}pq_p(2) + \frac{1}{2}pq_p(3) - \frac{1}{9}p^2q_p(2)^2 - \frac{1}{8}p^2q_p(3)^2 + \frac{1}{3}p^2q_p(2)q_p(3) + \frac{1}{72}p^2\left(\frac{3}{p}\right)B_{p-2}(\tfrac{1}{6})\right).$$

Since $p \equiv 1 \pmod 6$, we have $\left(\frac{3}{p}\right) = 1$. Also, using the identity

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots,$$

valid for $x \in p\mathbb{Z}_p$ we get

$$\frac{1}{1 + \frac{1}{2}pq_p(3) - \frac{1}{8}p^2q_p(3)^2 + \frac{1}{36}p^2B_{p-2}(\frac{1}{3})} \equiv 1 - \frac{1}{2}pq_p(3) + \frac{3}{8}p^2q_p(3)^2 - \frac{1}{36}p^2B_{p-2}(\tfrac{1}{3}) \pmod{p^3}.$$

We then have

$$\begin{aligned}\binom{\frac{p-1}{3}}{\frac{p-1}{6}} &\equiv (-1)^{\frac{p-1}{6}+1}\left(u_3 - \frac{p}{u_3} - \frac{p^2}{u_3^3}\right) \\ &\quad \times \left(1 + \frac{2}{3}pq_p(2) + \frac{1}{2}pq_p(3) - \frac{1}{9}p^2q_p(2)^2 - \frac{1}{8}p^2q_p(3)^2 + \frac{1}{3}p^2q_p(2)q_p(3)\right. \\ &\quad \left. + \frac{1}{72}p^2B_{p-2}\left(\tfrac{1}{6}\right)\right)\left(1 - \frac{1}{2}pq_p(3) + \frac{3}{8}p^2q_p(3)^2 - \frac{1}{36}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \\ &\equiv (-1)^{\frac{p-1}{6}+1}\left(u_3 - \frac{p}{u_3} - \frac{p^2}{u_3^3}\right) \\ &\quad \times \left(1 + \frac{2}{3}pq_p(2) - \frac{1}{9}p^2q_p(2)^2 - \frac{1}{36}p^2B_{p-2}\left(\tfrac{1}{3}\right) + \frac{1}{72}B_{p-2}\left(\tfrac{1}{6}\right)\right) \pmod{p^3}.\end{aligned}$$

We can further simplify this congruence by using the following lemma, which can be found on [32, page 158].

Lemma 3.1. *If $p \geq 5$, then* $5B_{p-2}\left(\frac{1}{3}\right) \equiv B_{p-2}\left(\frac{1}{6}\right) \pmod p$.

Using this lemma, we get an analogue to Theorem 1.3:

Theorem 3.2. *With p and u_3 as in* (3.1)–(3.2)*, we have*

$$\begin{aligned}\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv &(-1)^{\frac{p-1}{6}+1}\left(u_3 - \frac{p}{u_3} - \frac{p^2}{u_3^3}\right)\\ &\times\left(1 + \frac{2}{3}pq_p(2) - \frac{1}{9}p^2q_p(2)^2 + \frac{1}{24}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.\end{aligned}$$

3.1.2 The binomial coefficient $\binom{\frac{p-1}{2}}{\frac{p-1}{6}}$

In [1] we find the following two congruences:

$$\binom{\frac{p-1}{2}}{\frac{p-1}{6}} \equiv -2a_3 \pmod{p}.$$

$$\binom{\frac{p-1}{2}}{\frac{p-1}{6}} \equiv \left(2a_3 - \frac{p}{2a_3}\right)\left(-1 + \frac{2^p-2}{3} - \frac{3^p-3}{4}\right) \pmod{p^2}.$$

We will begin by obtaining an analogue to Theorem 1.4. From [1, Table 3.1.2] we have

$$J(\chi^2, \chi) = a_3 + ib_3\sqrt{3},$$

$$J(\chi^5, \chi^4) = a_3 - ib_3\sqrt{3}.$$

Furthermore, if $\mathfrak{p}$ is a nonzero prime ideal in the ring $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ of integers of $\mathbb{Q}(i\sqrt{3})$ dividing the prime p, then by [1, Theorem 2.1.14], we have

$$J(\chi^2, \chi) \equiv 0 \pmod{\mathfrak{p}}. \tag{3.4}$$

By taking $a = 1$ and $b = 2$ in Corollary 2.1, we obtain

$$J(\chi^5, \chi^4) = \frac{\Gamma_p(1-\frac{1}{2})}{\Gamma_p(1-\frac{1}{6})\Gamma_p(1-\frac{1}{3})}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^5, \chi^4) \equiv \frac{\Gamma_p(1+\frac{p^\alpha-1}{2})}{\Gamma_p(1+\frac{p^\alpha-1}{6})\Gamma_p(1+\frac{p^\alpha-1}{3})} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^5,\chi^4) \equiv \frac{F(1+\frac{p^\alpha-1}{2})}{F(1+\frac{p^\alpha-1}{6})F(1+\frac{p^\alpha-1}{3})} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^5,\chi^4) \equiv -\frac{(\frac{p^\alpha-1}{2})_p!}{(\frac{p^\alpha-1}{6})_p!(\frac{p^\alpha-1}{3})_p!} \pmod{p^\alpha}.$$

Next, (3.4) implies that $J(\chi^2,\chi)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}$. Thus

$$(a_3 + ib_3\sqrt{3})^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

Since this holds for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ dividing the prime p, we may conclude that this congruence also holds modulo p^α. We now expand the left-hand side and separate real and imaginary parts to obtain

$$-ib_3\sqrt{3}\sum_{j=0}^{\lfloor\frac{\alpha-1}{2}\rfloor}\binom{\alpha}{2j+1}(-1)^j a_3^{\alpha-2j-1}3^j b_3^{2j} \equiv \sum_{j=0}^{\lfloor\frac{\alpha}{2}\rfloor}\binom{\alpha}{2j}(-1)^j a_3^{\alpha-2j}3^j b_3^{2j} \pmod{p^\alpha}.$$

Because of the relationship $p = a_3^2 + 3b_3^2$, the first sum, S_3, becomes

$$S_3 = (2a_3)^{\alpha-1}\sum_{\nu=0}^{\lfloor\frac{\alpha-1}{2}\rfloor}\binom{\alpha-1-\nu}{\nu}\left(\frac{-p}{4a_3^2}\right)^\nu,$$

and the second sum, S_4, becomes

$$S_4 = \frac{1}{2}(2a_3)^\alpha\sum_{\nu=0}^{\lfloor\frac{\alpha}{2}\rfloor}\binom{\alpha-\nu}{\nu}\frac{\alpha}{\alpha-\nu}\left(\frac{-p}{4a_3^2}\right)^\nu.$$

Here we have used [18, Identities (3.120) and (3.121)] with $\nu = j-k$. Analogously to the previous section, we state:

Claim. *With p, a_3, and b_3 as described in* (3.1)–(3.2)*, we have*

$$-ib_3\sqrt{3} \equiv \frac{S_4}{S_3} \equiv a_3 + 2a_3 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \left(\frac{-p}{4a_3^2}\right)^j \pmod{p^\alpha}.$$

Putting everything back together we get another analogue to Theorem 1.4:

Theorem 3.3. *With p and a_3 as described in* (3.1)–(3.2)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(\frac{p^\alpha-1}{2})_p!}{(\frac{p^\alpha-1}{6})_p!(\frac{p^\alpha-1}{3})_p!} \equiv -2a_3 - 2a_3 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \left(\frac{-p}{4a_3^2}\right)^j \pmod{p^\alpha}.$$

To obtain our analogue to Theorem 1.3, we translate the congruence in Theorem 3.3 into a congruence involving binomial coefficients. From the previous section we have

$$\left(\frac{p^3-1}{3}\right)_p! \equiv (p-1)!^{\frac{p^2-1}{3}} \left(\frac{p-1}{3}\right)! \times \left(1 + \frac{1}{2}pq_p(3) - \frac{1}{8}p^2q_p(3)^2 + \frac{1}{36}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}$$

and

$$\left(\frac{p^3-1}{6}\right)_p! \equiv (p-1)!^{\frac{p^2-1}{6}} \left(\frac{p-1}{6}\right)! \left(1 + \frac{1}{3}pq_p(2) + \frac{1}{4}pq_p(3) - \frac{1}{9}p^2q_p(2)^2 - \frac{3}{32}p^2q_p(3)^2 + \frac{1}{12}p^2q_p(2)q_p(3) + \frac{1}{144}p^2\left(\frac{3}{p}\right)B_{p-2}\left(\tfrac{1}{6}\right)\right) \pmod{p^3}.$$

From [7] we have

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

Combining everything, we get another analogue to Theorem 1.3:

Theorem 3.4. *With p and a_3 as in* (3.1)–(3.2)*, we have*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{6}} \equiv \left(-2a_3 + \frac{p}{2a_3} + \frac{p^2}{8a^3}\right)\left(1 - \frac{2}{3}pq_p(2) + \frac{3}{4}pq_p(3) + \frac{5}{9}p^2q_p(2)^2 - \frac{3}{32}p^2q_p(3)^2 - \frac{1}{2}p^2q_p(2)q_p(3) + \frac{1}{16}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.$$

3.1.3 The binomial coefficient $\binom{\frac{2(p-1)}{3}}{\frac{p-1}{6}}$

In [1] we find the following two congruences:

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1}2a_3 \pmod{p}.$$

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}}\left(2a_3 - \frac{p}{2a_3}\right)\left(-1 - \frac{2(2^p-2)}{3} + \frac{3^p-3}{4}\right) \pmod{p^2}.$$

We will begin by obtaining an analogue to Theorem 1.4. From [1, Table 3.1.2] we have

$$J(\chi, \chi^3) = (-1)^{\frac{p-1}{6}}(a_3 + ib_3\sqrt{3}),$$

$$J(\chi^5, \chi^3) = (-1)^{\frac{p-1}{6}}(a_3 - ib_3\sqrt{3}).$$

Furthermore, if $\mathfrak{p}$ is a nonzero prime ideal in the ring $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ of integers of $\mathbb{Q}(i\sqrt{3})$ dividing the prime p, then by [1, Theorem 2.1.14], we have

$$J(\chi, \chi^3) \equiv 0 \pmod{\mathfrak{p}}. \tag{3.5}$$

By taking $a = 1$ and $b = 3$ in Corollary 2.1, we obtain

$$J(\chi^5, \chi^3) = \frac{\Gamma_p(1-\frac{2}{3})}{\Gamma_p(1-\frac{1}{6})\Gamma_p(1-\frac{1}{2})}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^5, \chi^3) \equiv \frac{\Gamma_p(1+\frac{2(p^\alpha-1)}{3})}{\Gamma_p(1+\frac{p^\alpha-1}{6})\Gamma_p(1+\frac{p^\alpha-1}{2})} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^5,\chi^3) \equiv \frac{F(1+\frac{2(p^\alpha-1)}{3})}{F(1+\frac{p^\alpha-1}{6})F(1+\frac{p^\alpha-1}{2})} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^5,\chi^3) \equiv -\frac{(\frac{2(p^\alpha-1)}{3})_p!}{(\frac{p^\alpha-1}{6})_p!(\frac{p^\alpha-1}{2})_p!} \pmod{p^\alpha}.$$

Next, (3.5) implies that $J(\chi,\chi^3)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}$. Thus

$$(a_3 + ib_3\sqrt{3})^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

Since this holds for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ dividing the prime p, we may conclude that this congruence also holds modulo p^α. We now expand the left-hand side and separate real and imaginary parts to obtain

$$-ib_3\sqrt{3}\sum_{j=0}^{\lfloor\frac{\alpha-1}{2}\rfloor}\binom{\alpha}{2j+1}(-1)^j a_3^{\alpha-2j-1}3^j b_3^{2j} \equiv \sum_{j=0}^{\lfloor\frac{\alpha}{2}\rfloor}\binom{\alpha}{2j}(-1)^j a_3^{\alpha-2j}3^j b_3^{2j} \pmod{p^\alpha}.$$

Because of the relationship $p = a_3^2 + 3b_3^2$, the first sum, S_5, becomes

$$S_5 = (2a_3)^{\alpha-1}\sum_{\nu=0}^{\lfloor\frac{\alpha-1}{2}\rfloor}\binom{\alpha-1-\nu}{\nu}\left(\frac{-p}{4a_3^2}\right)^\nu,$$

and the second sum, S_6, becomes

$$S_6 = \frac{1}{2}(2a_3)^\alpha\sum_{\nu=0}^{\lfloor\frac{\alpha}{2}\rfloor}\binom{\alpha-\nu}{\nu}\frac{\alpha}{\alpha-\nu}\left(\frac{-p}{4a_3^2}\right)^\nu.$$

Here we have used [18, Identities (3.120) and (3.121)] and set $\nu = j-k$. Analogously to the previous section, we state:

Claim. *With p, a_3, and b_3 as described in* (3.1)–(3.2)*, we have*

$$-ib_3\sqrt{3} \equiv \frac{S_6}{S_5} \equiv a_3 + 2a_3 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \left(\frac{-p}{4a_3^2}\right)^j \pmod{p^\alpha}.$$

Putting everything back together we get an analogue to Theorem 1.4:

Theorem 3.5. *With p and a_3 as described in* (3.1)–(3.2)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(\frac{2(p^\alpha-1)}{3})_p!}{(\frac{p^\alpha-1}{6})_p!(\frac{p^\alpha-1}{2})_p!} \equiv (-1)^{\frac{p-1}{6}+1} \left(2a_3 + 2a_3 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \left(\frac{-p}{4a_3^2}\right)^j\right) \pmod{p^\alpha}.$$

To obtain an analogue to Theorem 1.3, we translate the congruence in Theorem 3.5 into a congruence involving binomial coefficients.

We use our previous identities and Lemmas 2.4 and 2.5 to get

$$\left(\frac{2(p^3-1)}{3}\right)_p ! \equiv (p-1)!^{\frac{2(p^2-1)}{3}} \left(\frac{2(p-1)}{3}\right)! \left(1 + pq_p(3) - \frac{1}{9}p^2 B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.$$

From the previous sections we know that

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

and

$$\left(\frac{p^3-1}{6}\right)_p ! \equiv (p-1)!^{\frac{p^2-1}{6}} \left(\frac{p-1}{6}\right)! \left(1 + \frac{1}{3}pq_p(2) + \frac{1}{4}pq_p(3) - \frac{1}{9}p^2 q_p(2)^2 \right.$$
$$\left. -\frac{3}{32}p^2 q_p(3)^2 + \frac{1}{12}p^2 q_p(2)q_p(3) + \frac{1}{144}p^2 \left(\frac{3}{p}\right) B_{p-2}\left(\tfrac{1}{6}\right)\right) \pmod{p^3}.$$

Combining everything, in analogy to Theorem 1.3, we get:

Theorem 3.6. *With p and a_3 as described in* (3.1)–(3.2)*, we have*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1}\left(2a_3 - \frac{p}{2a_3} - \frac{p^2}{8a^3}\right)\left(1 + \frac{4}{3}pq_p(2) - \frac{3}{4}pq_p(3) + \frac{2}{9}p^2q_p(2)^2 + \frac{21}{32}p^2q_p(3)^2 - p^2q_p(2)q_p(3) + \frac{7}{48}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.$$

3.1.4 The binomial coefficient $\binom{p-1}{\frac{p-1}{3}}$

In [1] we find the following two congruences:

$$\binom{p-1}{\frac{p-1}{3}} \equiv 1 \pmod{p}.$$

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

We will begin by obtaining an analogue to Theorem 1.4. From [1, Table 3.1.2] we have

$$J(\chi^4, \chi^2) = -1.$$

By taking $a = 2$ and $b = 4$ in Corollary 2.1, we obtain

$$J(\chi^4, \chi^2) = \frac{\Gamma_p(1-1)}{\Gamma_p(1-\frac{1}{3})\Gamma_p(1-\frac{2}{3})}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^4, \chi^2) \equiv \frac{\Gamma_p(1+p^\alpha-1)}{\Gamma_p(1+\frac{p^\alpha-1}{3})\Gamma_p(1+\frac{2(p^\alpha-1)}{3})} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^4, \chi^2) \equiv \frac{F(1+p^\alpha-1)}{F(1+\frac{p^\alpha-1}{3})F(1+\frac{2(p^\alpha-1)}{2})} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^5,\chi^3) \equiv -\frac{(p^\alpha-1)_p!}{(\frac{p^\alpha-1}{3})_p!(\frac{2(p^\alpha-1)}{3})_p!} \pmod{p^\alpha}.$$

In analogy to Theorem 1.4, we get:

Theorem 3.7. *With p as described in* (3.1)–(3.2)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(p^\alpha-1)_p!}{(\frac{p^\alpha-1}{3})_p!(\frac{2(p^\alpha-1)}{3})_p!} \equiv 1 \pmod{p^\alpha}.$$

To obtain an analogue to Theorem 1.3, we translate the above congruence into a congruence involving binomial coefficients. Using the identities from previous sections we have the following analogue to Theorem 1.3:

Theorem 3.8. *With p as described in* (3.1)–(3.2)*, we have*

$$\binom{p-1}{\frac{p-1}{3}} \equiv 1 + \frac{3}{2}pq_p(3) + \frac{3}{8}p^2q_p(3)^2 - \frac{1}{12}p^2B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p^3}.$$

3.1.5 The binomial coefficient $\binom{p-1}{\frac{p-1}{6}}$

In [1] we find the following two congruences:

$$\binom{p-1}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}} \pmod{p}.$$

$$\binom{p-1}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}}\left(1 + (2^p-2) + \frac{3^p-3}{2}\right) \pmod{p^2}.$$

We will begin by obtaining an analogue to Theorem 1.4. From [1, Table 3.1.2] we have

$$J(\chi^5,\chi^1) = -(-1)^{\frac{p-1}{6}}.$$

By taking $a = 1$ and $b = 5$ in Corollary 2.1, we obtain

$$J(\chi^5,\chi) = \frac{\Gamma_p(1-1)}{\Gamma_p(1-\frac{1}{6})\Gamma_p(1-\frac{5}{6})}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^5, \chi^1) \equiv \frac{\Gamma_p(1+p^\alpha-1)}{\Gamma_p(1+\frac{p^\alpha-1}{6})\Gamma_p(1+\frac{5(p^\alpha-1)}{6})} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^5, \chi^1) \equiv \frac{F(1+p^\alpha-1)}{F(1+\frac{p^\alpha-1}{6})F(1+\frac{5(p^\alpha-1)}{6})} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^5, \chi^1) \equiv -\frac{(p^\alpha-1)_p!}{(\frac{p^\alpha-1}{6})_p!(\frac{5(p^\alpha-1)}{6})_p!} \pmod{p^\alpha}.$$

In analogy to Theorem 1.4, we have:

Theorem 3.9. *With p as described in* (3.1)–(3.2)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(p^\alpha-1)_p!}{(\frac{p^\alpha-1}{6})_p!(\frac{5(p^\alpha-1)}{6})_p!} \equiv (-1)^{\frac{p-1}{6}} \pmod{p^\alpha}.$$

To obtain our analogue to Theorem 1.3, we translate the above congruence into a congruence involving binomial coefficients. We use the same methods of the previous sections and Lemma 2.11 to get

$$\left(\frac{5(p^3-1)}{6}\right)_p! \equiv (p-1)!^{\frac{5(p^2-1)}{6}} \left(\frac{5(p-1)}{6}\right)! \left(1+\frac{5}{3}pq_p(2)+\frac{5}{4}pq_p(3)+\frac{5}{9}p^2q_p(2)^2 + \frac{5}{32}p^2q_p(3)^2+\frac{25}{12}p^2q_p(2)q_p(3)-\frac{125}{144}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.$$

Putting everything together we get, in analogy to Theorem 1.3, the following:

Theorem 3.10. *With p as in* (3.1)–(3.2)*, we have*

$$\binom{p-1}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}} \left(1+2pq_p(2)+\frac{3}{2}pq_p(3)+p^2q_p(2)^2 + \frac{3}{8}p^2q_p(3)^2+3p^2q_p(2)q_p(3)-\frac{5}{6}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.$$

3.1.6 The binomial coefficient $\binom{\frac{5(p-1)}{6}}{\frac{p-1}{3}}$

In [1] we find the following two congruences:

$$\binom{\frac{5(p-1)}{6}}{\frac{p-1}{3}} \equiv -2a_3 \pmod{p}.$$

$$\binom{\frac{5(p-1)}{6}}{\frac{p-1}{3}} \equiv \left(2a_3 - \frac{p}{2a_3}\right)\left(-1 + \frac{2^p-2}{3} + \frac{3^p-3}{4}\right) \pmod{p^2}.$$

We will begin by obtaining an analogue to Theorem 1.4. From [1, Table 3.1.2] we have

$$J(\chi^2, \chi^3) = a_3 + ib_3\sqrt{3},$$

$$J(\chi^4, \chi^3) = a_3 - ib_3\sqrt{3}.$$

Furthermore, if $\mathfrak{p}$ is a nonzero prime ideal in the ring $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ of integers of $\mathbb{Q}(i\sqrt{3})$ dividing the prime p, then by [1, Theorem 2.1.14], we have

$$J(\chi^2, \chi^3) \equiv 0 \pmod{\mathfrak{p}}. \tag{3.6}$$

By taking $a = 2$ and $b = 3$ in Corollary 2.1, we have

$$J(\chi^4, \chi^3) = \frac{\Gamma_p(1-\frac{5}{6})}{\Gamma_p(1-\frac{1}{3})\Gamma_p(1-\frac{1}{2})}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^4, \chi^3) = \frac{\Gamma_p(1+\frac{5(p^\alpha-1)}{6})}{\Gamma_p(1+\frac{p^\alpha-1}{3})\Gamma_p(1+\frac{p^\alpha-1}{2})} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^4, \chi^3) = \frac{F(1+\frac{5(p^\alpha-1)}{6})}{F(1+\frac{p^\alpha-1}{3})F(1+\frac{p^\alpha-1}{2})} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^4,\chi^3) \equiv -\frac{(\frac{5(p^\alpha-1)}{6})_p!}{(\frac{p^\alpha-1}{3})_p!(\frac{p^\alpha-1}{2})_p!} \pmod{p^\alpha}.$$

Next, (3.6) implies that $J(\chi^2,\chi^3)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}$. Thus

$$(a_3 + ib_3\sqrt{3})^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

Since this holds for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ dividing the prime p, we may conclude that this congruence also holds modulo p^α. We now expand the left-hand side and separate real and imaginary parts to obtain

$$-ib_3\sqrt{3}\sum_{j=0}^{\lfloor\frac{\alpha-1}{2}\rfloor}\binom{\alpha}{2j+1}(-1)^j a_3^{\alpha-2j-1}3^j b_3^{2j} \equiv \sum_{j=0}^{\lfloor\frac{\alpha}{2}\rfloor}\binom{\alpha}{2j}(-1)^j a_3^{\alpha-2j}3^j b_3^{2j} \pmod{p^\alpha}.$$

Because of the relationship $p = a_3^2 + 3b_3^2$, the first sum, S_7, becomes

$$S_7 = (2a_3)^{\alpha-1}\sum_{\nu=0}^{\lfloor\frac{\alpha-1}{2}\rfloor}\binom{\alpha-1-\nu}{\nu}\left(\frac{-p}{4a_3^2}\right)^\nu,$$

and the second sum, S_8, becomes

$$S_8 = \frac{1}{2}(2a_3)^\alpha\sum_{\nu=0}^{\lfloor\frac{\alpha}{2}\rfloor}\binom{\alpha-\nu}{\nu}\frac{\alpha}{\alpha-\nu}\left(\frac{-p}{4a_3^2}\right)^\nu.$$

Here we have used [18, Identities (3.120) and (3.121)] with $\nu = j-k$. Analogously to previous sections, we state:

Claim. *With p, a_3, and b_3 as described in* (3.1)–(3.2)*, we have*

$$-ib_3\sqrt{3} \equiv \frac{S_8}{S_7} \equiv a_3 + 2a_3\sum_{j=1}^{\alpha-1}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{4a_3^2}\right)^j \pmod{p^\alpha}.$$

Putting everything back together, we get an analogue to Theorem 1.4:

Theorem 3.11. *With p and a_3 as described in* (3.1)–(3.2)*, $\alpha \in \mathbb{N}$, we have*

$$\frac{(\frac{5(p^\alpha-1)}{6})_p!}{(\frac{p^\alpha-1}{3})_p!(\frac{p^\alpha-1}{2})_p!} \equiv 2a_3 + 2a_3 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \left(\frac{-p}{4a_3^2}\right)^j \pmod{p^\alpha}.$$

Using the identities for Gauss factorials from the previous sections and the following congruence:

$$\begin{aligned}
&\frac{1}{1+\frac{5}{3}pq_p(2)+\frac{5}{4}pq_p(3)+\frac{5}{9}p^2q_p(2)^2+\frac{5}{32}p^2q_p(3)^2+\frac{25}{12}p^2q_p(2)q_p(3)-\frac{125}{144}p^2B_{p-2}(\frac{1}{3})} \\
&\quad\equiv 1-\frac{5}{3}pq_p(2)-\frac{5}{4}pq_p(3)+\frac{20}{9}p^2q_p(2)^2+\frac{45}{32}p^2q_p(3)^2 \\
&\qquad+\frac{25}{12}p^2q_p(2)q_p(3)+\frac{125}{144}p^2B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p^3}
\end{aligned}$$

we get an analogue to Theorem 1.3.

Theorem 3.12. *With p and a_3 as described in* (3.1)–(3.2)*, we have*

$$\begin{aligned}
\binom{\frac{5(p-1)}{6}}{\frac{p-1}{3}} \equiv \left(-2a_3+\frac{p}{2a_3}+\frac{p^2}{8a_3^3}\right)&\left(1-\frac{2}{3}pq_p(2)-\frac{3}{4}pq_p(3)+\frac{5}{9}p^2q_p(2)^2\right. \\
&\left.+\frac{21}{32}p^2q_p(3)^2+\frac{1}{2}p^2q_p(2)q_p(3)+\frac{43}{48}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.
\end{aligned}$$

3.1.7 The binomial coefficient $\binom{\frac{5(p-1)}{6}}{\frac{p-1}{6}}$

In [1] we find the following two congruences:

$$\binom{\frac{5(p-1)}{6}}{\frac{p-1}{6}} \equiv -u_3 \pmod{p}.$$

$$\binom{\frac{5(p-1)}{6}}{\frac{p-1}{6}} \equiv \left(u_3-\frac{p}{u_3}\right)\left(-1+\frac{2(2^p-2)}{3}\right) \pmod{p^2}.$$

We will begin by obtaining an analogue to Theorem 1.4. From [1, Table 3.1.2] we have

$$J(\chi,\chi^4) = \frac{1}{2}(u_3 + iv_3\sqrt{3}),$$

$$J(\chi^5, \chi^2) = \frac{1}{2}(u_3 - iv_3\sqrt{3}).$$

Furthermore, if $\mathfrak{p}$ is a nonzero prime ideal in the ring $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ of integers of $\mathbb{Q}(i\sqrt{3})$ dividing the prime p, then by [1, Theorem 2.1.14], we have

$$J(\chi, \chi^4) \equiv 0 \pmod{\mathfrak{p}}. \tag{3.7}$$

By taking $a = 5$ and $b = 2$ in Corollary 2.1, we obtain

$$J(\chi^5, \chi^2) = \frac{\Gamma_p(1 - \frac{5}{6})}{\Gamma_p(1 - \frac{1}{6})\Gamma_p(1 - \frac{2}{3})}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^5, \chi^2) \equiv \frac{\Gamma_p(1 + \frac{5(p^\alpha - 1)}{6})}{\Gamma_p(1 + \frac{p^\alpha - 1}{6})\Gamma_p(1 + \frac{2(p^\alpha - 1)}{3})} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^5, \chi^2) \equiv \frac{F(1 + \frac{5(p^\alpha - 1)}{6})}{F(1 + \frac{p^\alpha - 1}{6})F(1 + \frac{2(p^\alpha - 1)}{3})} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^5, \chi^2) \equiv -\frac{(\frac{5(p^\alpha - 1)}{6})_p!}{(\frac{p^\alpha - 1}{6})_p!(\frac{2(p^\alpha - 1)}{3})_p!} \pmod{p^\alpha}.$$

Next, (3.7) implies that $J(\chi, \chi^4)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}$. Thus

$$\left(\frac{1}{2}u_3 + iv_3\sqrt{3}\right)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

Since this holds for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ dividing the prime p, we may conclude that this congruence also holds modulo p^α. We now expand the

left-hand side and separate real and imaginary parts to obtain

$$-iv_3\sqrt{3}\sum_{j=0}^{\lfloor\frac{\alpha-1}{2}\rfloor}\binom{\alpha}{2j+1}(-1)^j u_3^{\alpha-2j-1}3^j v_3^{2j} \equiv \sum_{j=0}^{\lfloor\frac{\alpha}{2}\rfloor}\binom{\alpha}{2j}(-1)^j u_3^{\alpha-2j}3^j v_3^{2j} \pmod{p^\alpha}.$$

Because of the relationship $3v_3^2 = 4p - u_3^2$, the first sum, S_9, becomes

$$S_9 = (2u_3)^{\alpha-1}\sum_{\nu=0}^{\lfloor\frac{\alpha-1}{2}\rfloor}\binom{\alpha-1-\nu}{\nu}\left(\frac{-p}{u_3^2}\right)^\nu,$$

and the second sum, S_{10}, becomes

$$S_{10} = \frac{1}{2}(2u_3)^\alpha\sum_{\nu=0}^{\lfloor\frac{\alpha}{2}\rfloor}\binom{\alpha-\nu}{\nu}\frac{\alpha}{\alpha-\nu}\left(\frac{-p}{u_3^2}\right)^\nu.$$

Here we have used [18, Identities (3.120) and (3.121)] with $\nu = j - k$. Analogously to previous sections, we state:

Claim. *With p, u_3, and v_3 as described in* (3.1)–(3.2)*, we have*

$$-iv_3\sqrt{3} \equiv \frac{S_{10}}{S_9} \equiv u_3 + 2u_3\sum_{j=1}^{\alpha-1}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}y^j \pmod{p^\alpha}.$$

Putting everything together we get the following analogue to Theorem 1.4:

Theorem 3.13. *With p and u_3 as described in* (3.1)–(3.2)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(\frac{5(p^\alpha-1)}{6})_p!}{(\frac{p^\alpha-1}{6})_p!(\frac{2(p^\alpha-1)}{3})_p!} \equiv u_3 + u_3\sum_{j=1}^{\alpha-1}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{u_3^2}\right)^j \pmod{p^\alpha}.$$

Using the identities for Gauss factorials from the previous sections, we have the following analogue to Theorem 1.3:

Theorem 3.14. *With p and u_3 as described in* (3.1)–(3.2)*, we have*

$$\binom{\frac{5(p-1)}{6}}{\frac{p-1}{6}} \equiv \left(-u_3 + \frac{p}{u_3} + \frac{p^2}{u_3^3}\right) \times \left(1 - \frac{4}{3}pq_p(2) + \frac{14}{9}p^2q_p(2)^2 + \frac{57}{72}p^2B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}.$$

3.1.8 The binomial coefficient $\binom{p-1}{\frac{p-1}{2}}$

In this section we give another method of proving a special case of Morley's congruence. From [1, Table 3.1.2] we have

$$J(\chi^3, \chi^3) = -(-1)^{\frac{p-1}{6}}.$$

By taking $a = b = 3$ in Corollary 2.1, we obtain

$$J(\chi^3, \chi^3) = \frac{\Gamma_p(1-1)}{(\Gamma_p(1-\frac{1}{2}))^2}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^3, \chi^3) \equiv \frac{\Gamma_p(1+p^\alpha-1)}{(\Gamma_p(1+\frac{p^\alpha-1}{2}))^2} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^3, \chi^3) \equiv \frac{F(1+p^\alpha-1)}{(F(1+\frac{p^\alpha-1}{2}))^2} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^3, \chi^3) \equiv -\frac{(p^\alpha-1)_p!}{((\frac{p^\alpha-1}{2})_p!)^2} \pmod{p^\alpha}.$$

Putting everything together we get the following analogue to Theorem 1.4:

Theorem 3.15. *With p as described in* (3.1)–(3.2)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(p^\alpha - 1)_p!}{((\frac{p^\alpha - 1}{2})_p!)^2} \equiv (-1)^{\frac{p-1}{6}} \pmod{p^\alpha}.$$

Using the identities for Gauss factorials from the previous sections and the definition of the Fermat quotient, we obtain the following special case of Morley's congruence:

Theorem 3.16. *With p as described in* (3.1)–(3.2)*, we have*

$$\binom{p-1}{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{6}} 4^{p-1} \pmod{p^3}.$$

This is not as general as Morley's congruence since we are restricted to primes $p \equiv 1 \pmod 6$; however, the two agree on primes congruent to 1 modulo 6.

3.2 The $p \equiv 1 \pmod 4$ case

Let $p = 4f + 1$ be a prime and let g be a primitive root modulo p. Define $\beta = \exp(\frac{2\pi i}{4}) = i$ and let χ be a character modulo p of order 4 such that $\chi(g) = \beta$. By Theorem 2.4 and the argument presented in Chapter 1, we can write

$$p = a_4^2 + b_4^2, \quad a_4 \equiv -\left(\frac{2}{p}\right) \pmod 4, \quad \text{and } b_4 \equiv a_4 g^{\frac{p-1}{4}}. \tag{3.8}$$

We will obtain several modulo p and modulo p^2 congruences in this section. The modulo p^2 ones can be obtained from [1, Theorem 9.4.3], and the modulo p ones can either be deduced from their modulo p^2 analogues, or can be found directly in [1, Theorem 9.2.2].

3.2.1 The binomial coefficient $\binom{p-1}{\frac{p-1}{2}}$

In this section we give a method of proving another special case of Morley's congruence. From [1, Table 3.2.1] we have

$$J(\chi^2, \chi^2) = -1.$$

By taking $a = b = 2$ in Corollary 2.1, we obtain

$$J(\chi^2, \chi^2) = \frac{\Gamma_p(1-1)}{\Gamma_p(1-\frac{1}{2})^2}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^2, \chi^2) \equiv \frac{\Gamma_p(1+p^\alpha-1)}{\Gamma_p(1+\frac{p^\alpha-1}{2})^2} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^2, \chi^2) \equiv \frac{F(1+p^\alpha-1)}{F(1+\frac{p^\alpha-1}{2})^2} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^2, \chi^2) = -\frac{(p^\alpha-1)_p!}{((\frac{p^\alpha-1}{2})_p!)^2} \pmod{p^\alpha}.$$

Putting everything together:

Theorem 3.17. *With p as described in* (3.8)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(p^\alpha-1)_p!}{((\frac{p^\alpha-1}{2})_p!)^2} \equiv 1 \pmod{p^\alpha}.$$

Using the identities for Gauss factorials from the previous sections and the definition of the Fermat quotient, we obtain the following special case of Morley's congruence:

Theorem 3.18. *With p as described in* (3.8)*, we have*

$$\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \pmod{p^3}.$$

This is not quite as general as Morley's congruence since we are restricted to primes $p \equiv 1 \pmod 4$; however, they agree on primes congruent to 1 modulo 4.

3.2.2 The binomial coefficient $\binom{p-1}{\frac{p-1}{4}}$

In [1] we find the following two congruences:

$$\binom{p-1}{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}} \pmod{p}.$$

$$\binom{p-1}{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}}(1+3(2^{p-1}-1)) \pmod{p^2}.$$

We will begin by obtaining an analogue to Theorem 1.4. From [1, Table 3.2.1] we have

$$J(\chi^3,\chi) = (-1)^{\frac{p-1}{4}}.$$

By taking $a = 1$ and $b = 3$ in Corollary 2.1, we obtain

$$J(\chi^3,\chi) = \frac{\Gamma_p(1-1)}{\Gamma_p(1-\frac{1}{4})\Gamma_p(1-\frac{3}{4})}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^3,\chi) \equiv \frac{\Gamma_p(1+p^\alpha-1)}{\Gamma_p(1+\frac{p^\alpha-1}{4})\Gamma_p(1+\frac{3(p^\alpha-1)}{4})} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^3,\chi) \equiv \frac{F(1+p^\alpha-1)}{F(1+\frac{p^\alpha-1}{4})F(1+\frac{3(p^\alpha-1)}{4})} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^3,\chi) \equiv -\frac{(p^\alpha-1)_p!}{(\frac{p^\alpha-1}{4})_p!(\frac{3(p^\alpha-1)}{4})_p!} \pmod{p^\alpha}.$$

Putting everything together:

Theorem 3.19. *With p as described in* (3.8)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(p^\alpha-1)_p!}{(\frac{p^\alpha-1}{4})_p!(\frac{3(p^\alpha-1)}{4})_p!} \equiv (-1)^{\frac{p-1}{4}} \pmod{p^\alpha}.$$

Using our identities for Gauss factorials from the previous sections and Lemma 2.10, we get

$$\left(\frac{3(p^3-1)}{4}\right)_p! \equiv (p-1)!^{\frac{3(p^2-1)}{4}} \left(\frac{3(p-1)}{4}\right)! \times \left(1+\frac{9}{4}pq_p(2)+\frac{45}{32}p^2q_p(2)^2-\frac{9}{8}p^2E_{p-3}\right) \pmod{p^3}.$$

We therefore have the following analogue of Theorem 1.3:

Theorem 3.20. *With p as described in* (3.8)*, we have*

$$\binom{p-1}{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}}(1+3pq_p(2)+3p^2q_p(2)^2-p^2E_{p-3}) \pmod{p^3}.$$

3.2.3 The binomial coefficient $\binom{\frac{3(p-1)}{4}}{\frac{p-1}{4}}$

In [1] we find the following two congruences:

$$\binom{\frac{3(p-1)}{4}}{\frac{p-1}{4}} \equiv -2a_4 \pmod{p}.$$

$$\binom{\frac{3(p-1)}{4}}{\frac{p-1}{4}} \equiv \left(2a_4-\frac{p}{2a_4}\right)\left(-1+\frac{2^{p-1}-1}{2}\right) \pmod{p^2}.$$

We will begin by obtaining an analogue to Theorem 1.4. From [1, Table 3.2.1] we

have

$$J(\chi, \chi^2) = a_4 + ib_4,$$

$$J(\chi^3, \chi^2) = a_4 - ib_4.$$

Furthermore, if $\mathfrak{p}$ is a nonzero prime ideal in the ring $\mathbb{Z}[i]$ of integers of $\mathbb{Q}(i)$ dividing the prime p, then by [1, Theorem 2.1.14], we have

$$J(\chi, \chi^2) \equiv 0 \pmod{\mathfrak{p}}. \tag{3.9}$$

By taking $a = 1$ and $b = 2$ in Corollary 2.1, we obtain

$$J(\chi^3, \chi^2) = \frac{\Gamma_p(1 - \frac{3}{4})}{\Gamma_p(1 - \frac{1}{4})\Gamma_p(1 - \frac{1}{2})}.$$

Let $\alpha \in \mathbb{N}$ be arbitrary. By applying Lemma 2.1, we know that

$$J(\chi^3, \chi^2) = \frac{\Gamma_p(1 + \frac{3(p^\alpha - 1)}{4})}{\Gamma_p(1 + \frac{p^\alpha - 1}{4})\Gamma_p(1 + \frac{p^\alpha - 1}{2})} \pmod{p^\alpha}.$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^3, \chi^2) = \frac{F(1 + \frac{3(p^\alpha - 1)}{4})}{F(1 + \frac{p^\alpha - 1}{4})F(1 + \frac{p^\alpha - 1}{2})} \pmod{p^\alpha}.$$

Comparing with the definition of the Gauss factorial, this gives

$$J(\chi^3, \chi^2) \equiv -\frac{(\frac{3(p^\alpha - 1)}{4})_p!}{(\frac{p^\alpha - 1}{4})_p!(\frac{p^\alpha - 1}{2})_p!} \pmod{p^\alpha}.$$

Next, (3.9) implies that $J(\chi, \chi^2)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}$. Thus

$$(a_4 + ib_4)^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

Since this holds for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}[i]$ dividing p, we may conclude that this congruence also holds modulo p^α. We now expand the left-hand side and

separate real and imaginary parts to obtain

$$-ib_4 \sum_{j=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha}{2j+1} (-1)^j a_4^{\alpha-2j-1} b_4^{2j} \equiv \sum_{j=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha}{2j} (-1)^j a_4^{\alpha-2j} b_4^{2j} \pmod{p^\alpha}.$$

Because of the relationship $p = a_4^2 + b_4^2$, the first sum, S_{11}, becomes

$$S_{11} = (2a_4)^{\alpha-1} \sum_{\nu=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \binom{\alpha-1-\nu}{\nu} \left(\frac{-p}{4a_3^2}\right)^\nu,$$

and the second sum, S_{12}, becomes

$$S_{12} = \frac{1}{2}(2a_4)^\alpha \sum_{\nu=0}^{\lfloor \frac{\alpha}{2} \rfloor} \binom{\alpha-\nu}{\nu} \frac{\alpha}{\alpha-\nu} \left(\frac{-p}{4a_4^2}\right)^\nu.$$

Here we have used [18, Identities (3.120) and (3.121)] with $\nu = j - k$. Analogously to previous sections, we state:

Claim. *With p, a_4, and b_4 as described in* (3.8)*, we have*

$$-ib_4 \equiv \frac{S_{12}}{S_{11}} \equiv a_4 + 2a_4 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \left(\frac{-p}{4a_4^2}\right)^j \pmod{p^\alpha}.$$

Putting everything together, we get the following analogue to Theorem 1.4:

Theorem 3.21. *With p and a_4 as described in* (3.8)*, and $\alpha \in \mathbb{N}$, we have*

$$\frac{(\frac{3(p^\alpha-1)}{4})_p!}{(\frac{p^\alpha-1}{4})_p!(\frac{p^\alpha-1}{2})_p!} \equiv -2a_4 - 2a_4 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \left(\frac{-p}{4a_4^2}\right)^j \pmod{p^\alpha}.$$

Using our identities for Gauss factorials from the previous sections as well as the congruence

$$\frac{1}{1 + \frac{9}{4}pq_p(2) + \frac{45}{32}p^2q_p(2)^2 - \frac{9}{8}p^2E_{p-3}} \equiv 1 - \frac{9}{4}pq_p(2) + \frac{117}{32}p^2q_p(2)^2 + \frac{9}{8}p^2E_{p-3} \pmod{p^3}$$

we get the following analogue to Theorem 1.3:

Theorem 3.22. *With p and a_4 as described in* (3.8)*, we have*

$$\binom{\frac{3(p-1)}{4}}{\frac{p-1}{4}} \equiv \left(-2a_4 + \frac{p}{2a_4} + \frac{p^2}{8a_4^3}\right)\left(1 - \frac{1}{2}pq_p(2) + \frac{3}{8}p^2q_p(2)^2 + \frac{5}{4}p^2E_{p-3}\right) \pmod{p^3}.$$

3.3 The $p \equiv 1 \pmod 8$ case

Let $p = 8f + 1$ be a prime and let g be a primitive root modulo p. Define $\beta = \exp(\frac{2\pi i}{8}) = \frac{1+i}{\sqrt{2}}$, and let χ be a character modulo p of order 8 such that $\chi(g) = \beta$.

As was done previously in this chapter with $p \equiv 1 \pmod 6$ and $p \equiv 1 \pmod 4$, we can get an analogue to Theorem 1.4. However, we cannot get a direct analogue to Theorem 1.3. From [1, Section 3.3] we have

$$J(\chi, \chi^7) = -(-1)^{\frac{p-1}{8}},$$

$$J(\chi^3, \chi^5) = -(-1)^{\frac{p-1}{8}}.$$

By taking $a = 7$, $b = 1$ and $a = 5$, $b = 3$ in Corollary 2.1, respectively, and then applying Lemma 2.1, we have, for every $\alpha \in \mathbb{N}$,

$$J(\chi^1, \chi^7) = \frac{\Gamma_p(1-1)}{\Gamma_p(1-\frac{7}{8})\Gamma_p(1-\frac{1}{8})} \equiv -\frac{(p^\alpha - 1)_p!}{(\frac{7(p^\alpha-1)}{8})_p!(\frac{p^\alpha-1}{8})_p!} \pmod{p^\alpha},$$

$$J(\chi^3, \chi^5) = \frac{\Gamma_p(1-1)}{\Gamma_p(1-\frac{5}{8})\Gamma_p(1-\frac{3}{8})} \equiv -\frac{(p^\alpha - 1)_p!}{(\frac{5(p^\alpha-1)}{8})_p!(\frac{3(p^\alpha-1)}{8})_p!} \pmod{p^\alpha}.$$

We now have our analogue to Theorem 1.4:

Theorem 3.23. *For primes $p \equiv 1 \pmod 8$ and $\alpha \in \mathbb{N}$, we have*

$$\frac{(p^\alpha - 1)_p!}{(\frac{7(p^\alpha-1)}{8})_p!(\frac{p^\alpha-1}{8})_p!} \equiv \frac{(p^\alpha - 1)_p!}{(\frac{5(p^\alpha-1)}{8})_p!(\frac{3(p^\alpha-1)}{8})_p!} \equiv (-1)^{\frac{p-1}{8}} \pmod{p^\alpha}.$$

The best we can do towards obtaining an analogue of Theorem 1.3 is depicted by the following two results. To simplify our notation we first make the following definitions:

Definition 3.1. *For primes* $p \equiv 1 \pmod 8$ *define*

$$S_1(p) := \sum_{j=1}^{\frac{p-1}{8}} \frac{1}{j}, \quad S_2(p) := \sum_{j=1}^{\frac{7(p-1)}{8}} \frac{1}{j}, \quad S_3(p) := \sum_{j=1}^{\frac{5(p-1)}{8}} \frac{1}{j}, \quad S_4(p) := \sum_{j=1}^{\frac{3(p-1)}{8}} \frac{1}{j}.$$

Definition 3.2. *For primes* $p \equiv 1 \pmod 8$ *define*

$$T_1(p) := \sum_{1 \le j < k \le \frac{p-1}{8}} \frac{1}{jk}, \quad T_2(p) := \sum_{1 \le j < k \le \frac{7(p-1)}{8}} \frac{1}{jk},$$
$$T_3(p) := \sum_{1 \le j < k \le \frac{5(p-1)}{8}} \frac{1}{jk}, \quad T_4(p) := \sum_{1 \le j < k \le \frac{3(p-1)}{8}} \frac{1}{jk}.$$

Definition 3.3. *For primes* $p \equiv 1 \pmod 8$ *define*

$$Q_1(p) := \sum_{j=1}^{\frac{p-1}{8}} \frac{1}{j^2}, \quad Q_2(p) := \sum_{j=1}^{\frac{7(p-1)}{8}} \frac{1}{j^2}, \quad Q_3(p) := \sum_{j=1}^{\frac{5(p-1)}{8}} \frac{1}{j^2}, \quad Q_4(p) := \sum_{j=1}^{\frac{3(p-1)}{8}} \frac{1}{j^2}.$$

We now specialize Theorem 3.23 to the case $\alpha = 3$, as was done in the previous sections, and obtain the following corollaries.

Corollary 3.1. *For primes* $p \equiv 1 \pmod 8$, *we have*

$$\binom{p-1}{\frac{p-1}{8}} \equiv (-1)^{\frac{p-1}{8}} \left(\left[1 - \frac{1}{8} p S_1(p) + \frac{1}{64} p^2 T_1(p) \right] \right)$$
$$\times \left(\left[1 - \frac{7}{8} p S_2(p) + \frac{49}{64} p^2 T_2(p) \right] \right) \pmod{p^3}.$$

Corollary 3.2. *For primes $p \equiv 1 \pmod 8$, we have*

$$\binom{p-1}{\frac{5(p-1)}{8}} \equiv (-1)^{\frac{p-1}{8}} \left(\left[1 - \frac{5}{8}pS_3(p) + \frac{25}{64}p^2T_3(p)\right]\right) \times \left(\left[1 - \frac{3}{8}pS_4(p) + \frac{9}{64}p^2T_4(p)\right]\right) \pmod{p^3}.$$

We note that the sums $S_1(p), \ldots, S_4(p)$; $T_1(p), \ldots, T_4(p)$; and $Q_1(p), \ldots, Q_4(p)$ that we have just defined are not independent. In fact, employing the same methods we used in Chapter 2, we have the following properties that relate the various sums to one another.

Lemma 3.2. *For primes $p \equiv 1 \pmod 8$, we have*

$$S_1(p) \equiv S_2(p) + pQ_2(p) \pmod{p^2},$$

$$S_3(p) \equiv S_4(p) + pQ_4(p) \pmod{p^2},$$

$$T_1(p) = \frac{1}{2}(S_1(p))^2 - \frac{1}{2}Q_1(p),$$

$$T_2(p) = \frac{1}{2}(S_2(p))^2 - \frac{1}{2}Q_2(p),$$

$$T_3(p) = \frac{1}{2}(S_3(p))^2 - \frac{1}{2}Q_3(p),$$

$$T_4(p) = \frac{1}{2}(S_4(p))^2 - \frac{1}{2}Q_4(p).$$

Chapter 4

Conclusion

We begin this final chapter with some direct consequences of the "first stage" results in Chapter 3, namely Theorem 3.1 and others. This is followed by some comments on questions related to Chapter 3, and by some remarks on possible further work. The main results of this thesis are then summarized in an appendix.

4.1 p-adic Expansions

In [7], Cosgrave and Dilcher state the following two corollaries of their main results.

Corollary 4.1. *Let χ, p and a be as in the statement of Theorem 1.3. Then we have the p-adic expansion*

$$J(\chi^3,\chi^3)=\frac{\Gamma_p(1-\frac{1}{2})}{\Gamma_p(1-\frac{1}{4})^2}=-2a+2a\sum_{j=1}^{\infty}\frac{1}{j}\binom{2j-2}{j-1}\left(\frac{p}{4a^2}\right)^j.$$

Corollary 4.2. *Let χ, p and r be as in the statement of Theorem 1.7. Then we have the p-adic expansion*

$$J(\chi^2,\chi^2)=\frac{\Gamma_p(1-\frac{2}{3})}{\Gamma_p(1-\frac{1}{3})^2}=r-r\sum_{j=1}^{\infty}\frac{1}{j}\binom{2j-2}{j-1}\left(\frac{p}{r^2}\right)^j.$$

Similarly, we can do the same with our results in Chapter 3. As a direct consequence of Theorems 3.1, 3.3, 3.5, 3.11, and 3.13 we have the following corollary:

Corollary 4.3. *Let χ, p, a_3, and u_3 be as described in* (3.1)–(3.2)*; then we have the*

$$J(\chi^5,\chi^5) = \frac{\Gamma_p(1-\frac{1}{3})}{\Gamma_p(1-\frac{1}{6})^2}$$
$$= (-1)^{f+1}\left(u_3 + u_3\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{u_3^2}\right)^j\right),$$

$$J(\chi^5,\chi^4) = \frac{\Gamma_p(1-\frac{1}{2})}{(\Gamma_p(1-\frac{1}{6}))(\Gamma_p(1-\frac{1}{3}))}$$
$$= 2a_3 + 2a_3\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{4a_3^2}\right)^j,$$

$$J(\chi^5,\chi^3) = \frac{\Gamma_p(1-\frac{2}{3})}{(\Gamma_p(1-\frac{1}{6}))(\Gamma_p(1-\frac{1}{2}))}$$
$$= (-1)^{\frac{p-1}{6}}\left(2a_3 + 2a_3\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{4a_3^2}\right)^j\right),$$

$$J(\chi^4,\chi^3) = \frac{\Gamma_p(1-\frac{5}{6})}{\Gamma_p(1-\frac{1}{3})\Gamma_p(1-\frac{1}{2})}$$
$$= 2a_3 + 2a_3\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{4a_3^2}\right)^j,$$

$$J(\chi^5,\chi^2) = \frac{\Gamma_p(1-\frac{5}{6})}{\Gamma_p(1-\frac{1}{6})\Gamma_p(1-\frac{2}{3})}$$
$$= u_3 + u_3\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{u_3^2}\right)^j.$$

Similarly, as a direct consequence of Theorem 3.21 we have the following corollary:

Corollary 4.4. *If $p \equiv 1 \pmod 4$, a_4, and χ are as described in* (3.8)*, then we have*

the p-adic expansion

$$J(\chi^3,\chi^2)=\frac{\Gamma_p(1-\frac{3}{4})}{\Gamma_p(1-\frac{1}{4})\Gamma_p(1-\frac{1}{2})}=-2a_4-2a_4\sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\left(\frac{-p}{4a_4^2}\right)^j.$$

4.2 Further Comments

We were not able to extend every congruence found in [1]. One of the major obstacles that prevented us from doing so was that we needed sums like the ones in Chapter 2 but for primes that are congruent to 1 modulo 5, 7, 8, 12, 14, 15, 16, 20, and 24. Another major obstacle we encountered when using the methods of Chapter 3 was that in the search for congruences for some binomial coefficients we were required to choose a and b in Corollary 2.1 in such a way that resulted in the evaluation of Γ_p at a negative argument.

There are many similarities between the results found in Chapter 3. This is perhaps not surprising, given that the congruences for finite sums we used to obtain our results share some similarities between them. For example, when considering primes congruent to 1 modulo 4 we saw the Euler numbers arise and when considering primes congruent to 1 modulo 6 we saw the Bernoulli polynomials arise exclusively.

As is mentioned by the authors in [7], further extensions modulo higher powers of the prime p may possibly be derived using their methods. However, as we increase α, the resulting congruences would become very complicated. There would also remain the issue of requiring more of the types of congruences for the finite sums used that are not in the literature.

Also, as is mentioned in [7], the numbers $B_{p-2}\left(\frac{1}{3}\right)$ and $B_{p-2}\left(\frac{1}{6}\right)$ that appear in our congruences are interesting on their own. They have connections to another sequence of numbers, Glaisher's G-numbers, denoted by $\{G_n\}$. The G-numbers are defined as

$G_n = (2n+1)I_n$ where I_n is the sequence

$$\frac{1}{e^x + e^{-x} + 1} = \frac{2}{3}\left(I_0 - \frac{I_1}{2!}x^2 + \frac{I_2}{4!}x^4 - \frac{I_3}{6!}x^6 + \dots\right).$$

These G-numbers are an analogue to the Euler numbers E_n and were studied by Glaisher in [17].

Binomial coefficients are our interest and are more familiar to most readers. However, Theorem 1.4 and its analogues look much more natural stated in terms of quotients of Gauss factorials rather than in terms of binomial coefficients.

Given the complexity of many of the congruences in Chapter 3, the theorems of Sections 3.1 and 3.2 were verified by computation with the computer algebra system Maple (Maple 17), for primes less than 200 and $\alpha \in \{1, 2, 3, 4\}$, where applicable.

A noticeable difference among the results of Chapter 3 involves the Catalan numbers; they appear in some of the congruences but not in all of them. It is clear from the respective proofs that the analogues of Theorem 1.4 that don't have the Catalan numbers in their expansion are exactly the ones where the Jacobi sums involved are equal to $\pm(-1)^f$.

4.3 Further Work

It would be ideal if we could extend every congruence found in [1], whether that involves finding new congruences for more finite sums and/or finding a new method that will help us work around Morita's p-adic Γ-function evaluated at negative arguments. We would also like to find applications for the congruences modulo p^3 that are obtained in Chapter 3.

Given the great degree of repetition in Chapter 3, it may be possible to combine all of the different proofs of Chapter 3 into one large proof. The main differences between the proofs is in the congruences for the Gauss factorials and the finite sums associated with each binomial coefficient.

4.4 Appendix: List of Congruences modulo p^3

For the convenience of the reader we have gathered all of the modulo p^3 congruences in the following two tables.

Let $p \equiv 1 \pmod 4$ be prime and let g be a primitive root modulo p. Define $\beta = \exp(\frac{2\pi i}{4}) = i$ and let χ be a character modulo p of order 4 such that $\chi(g) = \beta$. By Theorem 2.4 and the argument presented in Chapter 1, we can write $p^2 = a_4^2 + b_4^2$, where $a_4 \equiv -\left(\dfrac{2}{p}\right) \pmod 4$, and $b_4 \equiv a_4 g^{\frac{p-1}{4}}$. Then we have the following table.

Binomial Coeff.	Congruence modulo p^3
$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$	$\left(2a_4 - \frac{p}{2a_4} - \frac{p^2}{8a_4^3}\right)\left(1 + \frac{1}{2}pq_p(2) + \frac{1}{8}p^2\left(2E_{p-3} - q_p(2)^2\right)\right)$
$\binom{\frac{3(p-1)}{4}}{\frac{p-1}{4}}$	$\left(-2a_4 + \frac{p}{2a_4} + \frac{p^2}{8a_4^3}\right)\left(1 - \frac{1}{2}pq_p(2) + \frac{3}{8}p^2q_p(2)^2 + \frac{5}{4}p^2E_{p-3}\right)$
$\binom{p-1}{\frac{p-1}{4}}$	$(-1)^{\frac{p-1}{4}}\left(1 + 3pq_p(2) + 3p^2q_p(2)^2 - p^2E_{p-3}\right)$
$\binom{p-1}{\frac{p-1}{2}}$	4^{p-1}

Table 4.1: The case $p \equiv 1 \pmod 4$.

Let $p \equiv 1 \pmod 6$ be a prime and let g be a primitive root modulo p. Define $Z = \mathrm{ind}_g 2$, $\beta = \exp(\frac{2\pi i}{6})$, and χ is a character modulo p of order 6 such that $\chi(g) = \beta$. Then $p = a_3^2 + 3b_3^2$, where $a_3 \equiv -1 \pmod 3$, and $b_3 \equiv -Z \pmod 3$. By taking $u_3 = 2a_3$ and $v_3 = 2b_3$ we can also write $4p = u_3^2 + 3v_3^2$, where $u_3 \equiv 1 \pmod 3$, $v_3 \equiv Z \pmod 3$. Then we have the following table.

Binomial Coeff.	Congruence modulo p^3
$\binom{\frac{p-1}{3}}{\frac{p-1}{6}}$	$(-1)^{\frac{p-1}{6}+1}\left(u_3-\frac{p}{u_3}-\frac{p^2}{u_3^3}\right)\left(1+\frac{2}{3}pq_p(2)-\frac{1}{9}p^2q_p(2)^2+\frac{1}{24}p^2B_{p-2}\left(\frac{1}{3}\right)\right)$
$\binom{\frac{p-1}{2}}{\frac{p-1}{6}}$	$\left(-2a_3+\frac{p}{2a_3}+\frac{p^2}{8a^3}\right)\left(1-\frac{2}{3}pq_p(2)+\frac{3}{4}pq_p(3)+\frac{5}{9}p^2q_p(2)^2-\frac{3}{32}p^2q_p(3)^2-\frac{1}{2}p^2q_p(2)q_p(3)+\frac{1}{16}p^2B_{p-2}\left(\frac{1}{3}\right)\right)$
$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}}$	$\left(-r+\frac{p}{r}+\frac{p^2}{r^3}\right)\left(1+\frac{1}{6}p^2B_{p-2}\left(\frac{1}{3}\right)\right)$
$\binom{\frac{5(p-1)}{6}}{\frac{p-1}{6}}$	$\left(-u_3+\frac{p}{u_3}+\frac{p^2}{u_3^3}\right)\left(1-\frac{4}{3}pq_p(2)+\frac{14}{9}p^2q_p(2)^2+\frac{57}{72}p^2B_{p-2}\left(\frac{1}{3}\right)\right)$
$\binom{p-1}{\frac{p-1}{6}}$	$(-1)^{\frac{p-1}{6}}\left(1+2pq_p(2)+\frac{3}{2}pq_p(3)+p^2q_p(2)^2+\frac{3}{8}p^2q_p(3)^2+3p^2q_p(2)q_p(3)-\frac{5}{6}p^2B_{p-2}\left(\frac{1}{3}\right)\right)$
$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{6}}$	$(-1)^{\frac{p-1}{6}+1}\left(2a_3-\frac{p}{2a_3}-\frac{p^2}{8a^3}\right)\left(1+\frac{4}{3}pq_p(2)-\frac{3}{4}pq_p(3)+\frac{2}{9}p^2q_p(2)^2+\frac{21}{32}p^2q_p(3)^2-p^2q_p(2)q_p(3)+\frac{7}{48}p^2B_{p-2}\left(\frac{1}{3}\right)\right)$
$\binom{\frac{5(p-1)}{6}}{\frac{p-1}{6}}$	$\left(-u_3+\frac{p}{u_3}+\frac{p^2}{u_3^3}\right)\left(1-\frac{4}{3}pq_p(2)+\frac{14}{9}p^2q_p(2)^2+\frac{57}{72}p^2B_{p-2}\left(\frac{1}{3}\right)\right)$
$\binom{\frac{5(p-1)}{6}}{\frac{p-1}{3}}$	$\left(-2a_3+\frac{p}{2a_3}+\frac{p^2}{8a_3^3}\right)\left(1-\frac{2}{3}pq_p(2)-\frac{3}{4}pq_p(3)+\frac{5}{9}p^2q_p(2)^2+\frac{21}{32}p^2q_p(3)^2+\frac{1}{2}p^2q_p(2)q_p(3)+\frac{43}{48}p^2B_{p-2}\left(\frac{1}{3}\right)\right)$
$\binom{p-1}{\frac{p-1}{3}}$	$1+\frac{3}{2}pq_p(3)+\frac{3}{8}p^2q_p(3)^2-\frac{1}{12}p^2B_{p-2}\left(\frac{1}{3}\right)$
$\binom{p-1}{\frac{p-1}{2}}$	4^{p-1}

Table 4.2: The case $p\equiv 1 \pmod 6$.

Bibliography

[1] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi Sums*, volume 21 of *Canadian Mathematical Society Series of Monographs and Advanced Texts*. John Wiley and Sons, Inc., 1998.

[2] F. Beukers. Arithmetical properties of Picard-Fuchs equations. In *Seminar on number theory, Paris 1982-83*, volume 51 of *Progr. Math.*, pages 33–38. Birkhäuser, Boston, 1984.

[3] L. Carlitz. A theorem of Glaisher. *Canadian Journal of Mathematics*, 5:306–316, 1953.

[4] S. Chowla, B. Dwork, and R. Evans. On the mod p^2 determination of $\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$. *Journal of Number Theory*, 24(2):188–196, 1986.

[5] H. Cohen. *Number Theory Volume II: Analytic and Modern Tools*, volume 2. Springer, 2007.

[6] J. B. Cosgrave and K. Dilcher. Extensions of the Gauss-Wilson theorem. *Integers: Electronic Journal Of Combinatorial Number Theory*, 8, 2008.

[7] J. B. Cosgrave and K. Dilcher. Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients. *Acta Arithmetica*, 142(2):103–118, 2010.

[8] J. B. Cosgrave and K. Dilcher. An introduction to Gauss factorials. *American Mathematical Monthly*, 118(9):812–829, 2011.

[9] J. B. Cosgrave and K. Dilcher. The multiplicative orders of certain Gauss factorials. *International Journal of Number Theory*, 7(1):145–171, 2011.

[10] J. B. Cosgrave and K. Dilcher. The multiplicative orders of certain Gauss factorials, II. *Preprint*, 2014.

[11] E. Costa, R. Gerbicz, and D. Harvey. A search for Wilson primes. *ArXiv Mathematics e-prints*, 2012.

[12] D. A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. John Wiley and Sons, Inc., 1989.

[13] R. Crandall, K. Dilcher, and C. Pomerance. A search for Wieferich and Wilson primes. *Mathematics of Computation*, 66(217):433–449, January 1997.

[14] R. E. Crandall. *Topics in advanced scientific computation*. Springer-Verlag, New York, 1996.

[15] L. E. Dickson. *History of the Theory of Numbers. Volume I: Divisibility and Primality*. Chelsea, New York, 1971.

[16] F. G. Dorais and D. Klyve. A Wieferich prime search up to 6.7×10^{15}. *Journal of Integer Sequences*, 14(9):Article 11.9.2, 14, 2011.

[17] J. W. L. Glaisher. On a set of coefficients analogous to the Eulerian numbers. *Proceedings of the London Mathematical Society*, S1-31(1):215–235, 1899.

[18] H. W. Gould. *Combinatorial Identities*. Gould Publications, 1972.

[19] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics*. Addison-Wesley, 1994.

[20] A. Granville. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. In *Organic Mathematics)Burnaby, BC, 1995)*, volume 20 of *CMS Conference Proceedings*, pages 253–276. American Mathematical Society, Providence, RI, 1997.

[21] B. H. Gross and N. Koblitz. Gauss sums and the p-adic Γ-function. *Annals of Mathematics*, 109(3):569–581, 1979.

[22] R. H. Hudson and K. S. Williams. Binomial coefficients and Jacobi sums. *Transactions of the American Mathematical Society*, 281(2):431–505, February 1984.

[23] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1984.

[24] E. Lehmer. On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson. *Annals of Mathematics*, 39:350–360, 1938.

[25] F. Lemmermeyer. *Reciprocity Laws*. Springer Monographs in Mathematics. Springer, 2000.

[26] A. D. Loveless. A congruence for products of binomial coefficients modulo a composite. *Integers: Electronic Journal Of Combinatorial Number Theory*, 7, 2007.

[27] Y. Morita. A p-adic analogue of the Γ -function. *Journal of the Faculty of Science*, 22(2):255–266, 1975.

[28] F. Morley. Note on the congruence $2^{4n} \equiv (-1)^n(2n)/(n!)^2$, where $2n + 1$ is a prime. *Annals of Mathematics*, 9:168–170, 1895.

[29] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley and Sons, Inc., New York, fifth edition, 1991.

[30] F. W. J. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, editors. *NIST Handbook of Mathematical Functions*. U.S. Department of Commerce National Institute of Standards and Technology, 2010.

[31] G. Overholtzer. Sum functions in elementary p-adic analysis. *American Journal of Mathematics*, 74(2):332–346, 1952.

[32] P. Ribenboim. *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, 1979.

[33] Z. H. Sun. Congruences involving Bernoulli and Euler numbers. *Journal of Number Theory*, 128:280–312, 2008.