Gauss Sums and Multinomial Coefficients

Paul Thomas Young

Department of Mathematics, University of Charleston
Charleston, SC 29424

Consider a Gauss sum for a finite field of characteristic p, where p is an odd prime. When such a sum (or a product of such sums) is a p-adic integer we show how it can be realized as a p-adic limit of a sequence of multinomial coefficients. As an application we generalize some congruences of Hahn and Lee to exhibit p-adic limit formulae, in terms of multinomial coefficients, for certain algebraic integers in imaginary quadratic fields related to the splitting of rational primes. We also give an example illustrating how such congruences arise from a p-integral formal group law attached to the p-adic unit part of a product of Gauss sums.

Keywords. Gauss sums; multinomial coefficients, imaginary quadratic fields.

1. Introduction.

Suppose p is an odd prime of the form $p = tn + r$ which splits in the imaginary quadratic field $\mathbb{Q}(\sqrt{-t})$. Stickelberger [16] proved that if $t \notin \{3, 4, 8\}$ and $-t$ is a fundamental discriminant then there are integers a, b such that $4p^h = a^2 + tb^2$, where h is the class number of $\mathbb{Q}(\sqrt{-t})$. A classical problem is to characterize the integer a by congruence conditions. In the case where t is a prime, eight times a prime, or four times a prime of the form $4m + 1$, Lee and Hahn [15] used certain products of Gauss sums to determine a modulo t and express a modulo p as a product of binomial coefficients; in the case $h = 1$ these congruences already determine a exactly. In this paper we show how, since $\mathbb{Q}(\sqrt{-t}) \subset \mathbb{Q}_p$ if and only if p splits in $\mathbb{Q}(\sqrt{-t})$, such congruences may be extended to p-adic limit formulae for products of Gauss sums, and thus for the integer a, in terms of multinomial coefficients.

Early congruence results on this problem for $r = 1$ are due to Gauss [7] for $t = 4$ and to Jacobi [12], [13] for $t = 3, 7, 8$, along with later generalizations due to Hudson and Williams [11], Chowla, Dwork, and Evans [3], Coster [5], and Yeung [19]. These results all follow from calculations involving Jacobi sums over the prime field $\mathbb{F}_p$. Eisenstein [6] introduced Jacobi sums over $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ in order to treat the cases $p = 8n + 3$, $7n + 2$, and $7n + 4$, and indicated that these results could also be obtained using elliptic functions; see [1] for an account of how Eisenstein might have known this. One expects that such a connection to elliptic functions should in fact give rise to a

system of congruences for those Jacobi sums. In ([20], Theorem 2.2, Corollary 2.3) we gave systems of congruences implying p-adic limit formulae for Jacobi sums over arbitrary finite fields in terms of multinomial coefficients, which may be applied to this question.

Hahn and Lee [9] and Lee and Hahn [14] used Gauss sums over extensions of the prime field to obtain general congruences modulo p in certain cases where r generates a subgroup of index two in $(\mathbb{Z}/t\mathbb{Z})^\times$. In [15] they relaxed this restriction on r by considering suitable products of such Gauss sums. In the present paper we observe that these particular products of Gauss sums are in fact $\mathbb{Z}_p$-valued and therefore independent of the additive character, and that they may therefore be expressed as limits of multinomial coefficients by the methods of [20].

The $s = 1$ case of our congruences in Sections 3 and 4 imply the mod p congruences of [9], [14], [15]. While the congruences of [9], [14], [15] involve only the p-adic unit part of the associated Gauss sums, the multinomial coefficients of our congruences naturally express the p-adic ordinal of the Gauss sums, as well as their unit part. In Section 5 we consider the $t = 7$ example and adapt the method to isolate the p-adic unit part of the Gauss sums as a limit of products of binomial coefficients, extending the results given in the tables of [15]. In fact the congruences we give there provide an *ad hoc* construction of the invariant differential on a p-integral formal group law attached to the p-adic unit part of these Gauss sums. In light of the historical hypothesis of [1], it would be of interest to know how this differential might be related to elliptic functions.

2. Notations and Preliminaries.

Throughout this paper p will denote an odd prime, $\mathbb{F}_q$ the finite field of $q = p^f$ elements, $\mathbb{Z}_p$ the ring of p-adic integers, $\mathbb{Q}_p$ the field of p-adic numbers, and for any positive integer n, ζ_n will denote a fixed primitive n-th root of unity in some extension of $\mathbb{Q}_p$. We let π be a fixed solution in the ring of integers of $\mathbb{Q}_p(\zeta_p)$ to $\pi^{p-1} = -p$ chosen so that $\zeta_p \equiv 1 + \pi \pmod{(\pi^2)}$.

The Dwork shift map $\alpha \mapsto \alpha'$ on $\mathbb{Q} \bigcap \mathbb{Z}_p$ is defined by requiring that $p\alpha' - \alpha = \mu_\alpha \in \{0, 1, 2, ..., p-1\}$. We write $\alpha^{(0)} = \alpha$, and $\alpha^{(i)} = (\alpha^{(i-1)})'$ for $i > 0$; we also will write $\mu_\alpha^{(i)}$ for $\mu_{\alpha^{(i)}}$. It follows that the $\mu_\alpha^{(i)}$ are the digits in the p-adic expansion of $-\alpha$, that is, $-\alpha = \sum_{i=0}^{\infty} \mu_\alpha^{(i)} p^i$. It

is easy to verify that this map is well-defined and continuous; that $\alpha^{(i)} = 0$ for some i if and only if α is zero or a negative integer; and that $\alpha^{(f)} = \alpha$ if and only if α is a rational number in $[0,1]$ with denominator dividing $q-1$.

The Morita p-adic gamma function Γ_p is defined for positive integers n by

$$\Gamma_p(n) = (-1)^n \prod_{\substack{0<j<n \\ p \nmid j}} j, \tag{2.1}$$

and extends to a continuous function $\Gamma_p : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times$, which is Lipschitz with constant 1, and satisfies the functional equations of translation and reflection

$$\Gamma_p(x+1) = \begin{cases} -x\Gamma_p(x), & x \in \mathbb{Z}_p^\times, \\ -\Gamma_p(x), & x \in p\mathbb{Z}_p; \end{cases} \tag{2.2}$$

$$\Gamma_p(x)\Gamma_p(1-x) = -(-1)^{\mu_x}, \quad x \in \mathbb{Z}_p. \tag{2.3}$$

Let $\psi : \mathbb{F}_p \to \mathbb{Q}_p(\zeta_p)^\times$ be the additive character on $\mathbb{F}_p$ defined by $\psi(\bar{t}) = \zeta_p^t$, and let $\psi_f : \mathbb{F}_q \to \mathbb{Q}_p(\zeta_p)^\times$ denote the additive character on $\mathbb{F}_q$ defined by $\psi_f(t) = \psi(\mathrm{Tr}(t))$, where Tr: $\mathbb{F}_q \to \mathbb{F}_p$ is the trace map. The Teichmüller character $\omega_f : \mathbb{F}_q^\times \to \mathbb{Q}_p(\zeta_{q-1})^\times$ is the unique multiplicative character on $\mathbb{F}_q^\times$ such that, for all $t \in \mathbb{F}_q^\times$, the image of $\omega_f(t)$ in the residue-class field of $\mathbb{Q}_p(\zeta_{q-1})$ is t.

For $a \in \mathbb{Z}$, $0 \le a < q-1$, the Gauss sum $g(\omega_f^{-a})$ over $\mathbb{F}_q$ associated to the characters ψ_f and ω_f^{-a} is defined by

$$g(\omega_f^{-a}) \;=\; -\sum_{t \in \mathbb{F}_q^\times} \psi_f(t)\omega_f^{-a}(t). \tag{2.4}$$

By definition $g(\omega_f^{-a})$ is *a priori* an algebraic integer in $\mathbb{Q}(\zeta_p, \zeta_{q-1})$ and depends on the choice of ζ_p. The Gross-Koblitz formula [8] states that

$$g(\omega_f^{-a}) = \pi^{S(a)} \cdot \prod_{i=0}^{f-1} \Gamma_p(\alpha^{(i)}), \tag{2.5}$$

where $\alpha = a/(q-1)$ and $S(a)$ denotes the sum of the digits in the base p expansion of a. From this it is clear that $g(\omega_f^{-a}) \in \mathbb{Z}_p$ if and only if a is a multiple of $p-1$, and in this case $g(\omega_f^{-a})$ is independent of the choice of additive character (that is, independent of the choice of ζ_p and π).

In ([20], Lemma 2.1) we proved the following lemma, which will be used in section 3 to relate $\mathbb{Z}_p$-valued Gauss sums to multinomial coefficients via (2.5).

LEMMA 2.1. *Suppose $m_1, ..., m_s$ are nonnegative integers and write $m_j = k_j p + l_j$ with each $l_j \in \{0, 1, ..., p-1\}$; set $m = m_1 + \cdots + m_s$, $k = k_1 + \cdots + k_s$, and $l = l_1 + \cdots + l_s$. Let ε be a nonnegative integer and set $\delta = [\![(l+\varepsilon)/p]\!]$. Then*

$$\frac{(m+\varepsilon)!\, k_1! \cdots k_s!}{(k+\delta)!\, m_1! \cdots m_s!} = (-p)^{\delta} \frac{\Gamma_p(-m_1) \cdots \Gamma_p(-m_s)}{\Gamma_p(-m-\varepsilon)}.$$

Suppose that $t > 4$ is a positive integer and $-t$ is a fundamental discriminant. We identify the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_t)/\mathbb{Q})$ with $G = (\mathbb{Z}/t\mathbb{Z})^{\times}$ and let H be the subgroup of G corresponding to $\mathrm{Gal}(\mathbb{Q}(\zeta_t)/\mathbb{Q}(\sqrt{-t}))$; observe that H is a subgroup of index two in G that does not contain -1. Define the sums

$$c = \frac{1}{t} \sum_{\substack{0<i<t \\ i \in H}} i, \qquad d = \frac{1}{t} \sum_{\substack{0<i<t \\ -i \in H}} i. \tag{2.6}$$

Then c and d are integers (if $t \neq 8$) such that the class number h of $\mathbb{Q}(\sqrt{-t})$ is equal to $d - c$ (cf. ([4], Cor. 5.3.13)). Suppose that $p = tn + r$ is an odd prime with $r \in H$, and let $R = \{c_1, ..., c_g\} \subset H$ be a complete set of coset representatives of $H/\langle r \rangle$. According to Lee and Hahn ([15], Lemma 2.1), if f is the order of r in G and $q = p^f$, then the products of Gauss sums

$$\prod_{k=1}^{g} g(\omega_f^{-c_k(q-1)/t}) \qquad \text{and} \qquad \prod_{k=1}^{g} g(\omega_f^{c_k(q-1)/t}) \tag{2.7}$$

are independent of the choice of R and lie in $\mathbb{Q}(\sqrt{-t})$. For certain values of t (see §4) these products are related to the representation of $4p^h$ by binary quadratic forms.

3. Congruences for Gauss sums.

We first give an explicit formula which expresses any $\mathbb{Z}_p$-valued Gauss sum as a p-adic limit of ratios of multinomial coefficients.

THEOREM 3.1. *Suppose $0 \leq a < q-1$ and a is a multiple of $p-1$, and define $c = S(a)/(p-1)$. Define $\alpha = a/(q-1)$ and for $0 \leq i \leq f-1$ and $s \geq 0$ define the nonnegative integer $n_s^{(i)} = p^s \alpha^{(i+s)} - \alpha^{(i)}$, and put $n_s = \sum_{i=0}^{f-1} n_s^{(i)}$. Then for all $s > 0$ we have the congruence*

$$\frac{\binom{n_s + c}{n_s^{(0)}, ..., n_s^{(f-1)}, c}}{\binom{n_{s-1} + c}{n_{s-1}^{(0)}, ..., n_{s-1}^{(f-1)}, c}} \equiv g(\omega_f^{-a}) \pmod{p^{c+s}\mathbb{Z}_p}.$$

If in addition we have $c \le p$ then for all $s > 0$ we also have

$$p \cdot \frac{\binom{n_s}{n_s^{(0)}, \ldots, n_s^{(f-1)}}}{\binom{n_{s-1}}{n_{s-1}^{(0)}, \ldots, n_{s-1}^{(f-1)}}} \equiv g(\omega_f^{-a}) \pmod{p^{c+s}\mathbb{Z}_p}.$$

Proof. Recall that $\alpha^{(f)} = \alpha$ and $\mu_\alpha^{(f)} = \mu_\alpha$, and observe that $-n_s^{(i)} \equiv \alpha^{(i)} \pmod{p^s\mathbb{Z}_p}$ for all i, s. We compute

$$\begin{aligned} n_s &= \sum_{i=0}^{f-1} n_s^{(i)} = \sum_{i=0}^{f-1}\sum_{j=0}^{s-1} \mu_\alpha^{(i+j)} p^j \\ &= \sum_{j=0}^{s-1} p^j \sum_{i=0}^{f-1} \mu_\alpha^{(i+j)} = \sum_{j=0}^{s-1} p^j \cdot (p-1)c \\ &= c(p^s - 1), \end{aligned} \tag{3.1}$$

and therefore $n_s + c = cp^s \equiv 0 \pmod{p^s}$. Since $\Gamma_p(0) = 1$ and Γ_p is Lipschitz with constant 1, from the Gross-Koblitz formula we obtain

$$\begin{aligned} g(\omega_f^{-a}) &= (-p)^c \frac{\prod_{i=0}^{f-1} \Gamma_p(\alpha^{(i)})}{\Gamma_p(0)} \\ &\equiv (-p)^c \frac{\prod_{i=0}^{f-1} \Gamma_p(-n_s^{(i)})}{\Gamma_p(-n_s - c)} \pmod{p^{c+s}\mathbb{Z}_p}. \end{aligned} \tag{3.2}$$

Applying Lemma 2.1 with $m_i = n_s^{(i)}$, we have $k_i = n_{s-1}^{(i)}$ and $l_i = \mu_\alpha^{(i)}$, and taking $\varepsilon = \delta = c$, we find that the latter member of this congruence is precisely

$$\frac{\binom{n_s + c}{n_s^{(0)}, \ldots, n_s^{(f-1)}, c}}{\binom{n_{s-1} + c}{n_{s-1}^{(0)}, \ldots, n_{s-1}^{(f-1)}, c}}, \tag{3.3}$$

which completes the proof of the first statement. For the second statement, observe that

$$\frac{\binom{n_s + c}{n_s^{(0)}, \ldots, n_s^{(f-1)}, c}}{\binom{n_{s-1} + c}{n_{s-1}^{(0)}, \ldots, n_{s-1}^{(f-1)}, c}} = \frac{\binom{n_s}{n_s^{(0)}, \ldots, n_s^{(f-1)}}}{\binom{n_{s-1}}{n_{s-1}^{(0)}, \ldots, n_{s-1}^{(f-1)}}} \cdot \prod_{j=0}^{c-1} \left(\frac{cp^s - j}{cp^{s-1} - j} \right). \tag{3.4}$$

Comparing (3.2) and (3.3) shows that the left side of (3.4) has p-adic ordinal c, and if $c \le p$ the product factor on the right is congruent to p modulo p^s, so

$$\frac{\binom{n_s + c}{n_s^{(0)}, \ldots, n_s^{(f-1)}, c}}{\binom{n_{s-1} + c}{n_{s-1}^{(0)}, \ldots, n_{s-1}^{(f-1)}, c}} \equiv p \cdot \frac{\binom{n_s}{n_s^{(0)}, \ldots, n_s^{(f-1)}}}{\binom{n_{s-1}}{n_{s-1}^{(0)}, \ldots, n_{s-1}^{(f-1)}}} \pmod{p^{c+s}\mathbb{Z}_p}, \tag{3.5}$$

proving the second statement.

This proof may be modified to accomodate $\mathbb{Z}_p$-valued products of Gauss sums. We now give two such modifications of Theorem 3.1 which apply to the $\mathbb{Z}_p$-valued products of Gauss sums used by Lee and Hahn in [15]. We suppose p is an odd prime of the form $p = tn + r$ as described in section 2 and fix a set $R = \{c_1, ..., c_g\} \subset H$ of coset representatives of $H/\langle r \rangle$. While the individual Gauss sums appearing in (2.7) are not themselves $\mathbb{Z}_p$-valued in general, their product is $\mathbb{Z}_p$-valued and can be expressed as a p-adic limit of ratios of multinomial coefficients.

THEOREM 3.2. *Let $p = tn + r$ be an odd prime and let f be the order of r in $(\mathbb{Z}/t\mathbb{Z})^\times$. With notations as in Section 2, write $H = \{b_1, ..., b_{fg}\}$, set $\beta_l = b_l/t$, and define the nonnegative integer $n_{l,s} = p^s\beta_l^{(s)} - \beta_l$ for $1 \le l \le fg$ and $s \ge 0$. Let $n_s = \sum_{l=1}^{fg} n_{l,s}$ and define c as in (2.6). Then for all $s > 0$ we have the congruence*

$$\frac{\binom{n_s + c}{n_{1,s}, ..., n_{fg,s}, c}}{\binom{n_{s-1} + c}{n_{1,s-1}, ..., n_{fg,s-1}, c}} \equiv \prod_{k=1}^{g} g(\omega_f^{-c_k(q-1)/t}) \pmod{p^{c+s}\mathbb{Z}_p}.$$

If in addition we have $c \le p$ then for all $s > 0$ we also have

$$p \cdot \frac{\binom{n_s}{n_{1,s}, ..., n_{fg,s}}}{\binom{n_{s-1}}{n_{1,s-1}, ..., n_{fg,s-1}}} \equiv \prod_{k=1}^{g} g(\omega_f^{-c_k(q-1)/t}) \pmod{p^{c+s}\mathbb{Z}_p}.$$

Proof. By the Gross-Koblitz formula (2.5) we have

$$\prod_{k=1}^{g} g(\omega_f^{-c_k(q-1)/t}) = \pi^S \cdot \prod_{k=1}^{g} \prod_{i=0}^{f-1} \Gamma_p(\alpha_k^{(i)}), \tag{3.6}$$

where $S = \sum_{k=1}^{g} S(c_k(q-1)/t)$ and $\alpha_k = c_k/t$ for $k = 1, ..., g$. Observe that if $\alpha = s_0/t$ with $0 < s_0 < t$ then $\alpha' = s_1/t$ with $0 < s_1 < t$ and $rs_1 \equiv s_0 \pmod{t}$. It follows that for $k = 1, ..., g$ the set $\{\alpha_k, \alpha_k', ..., \alpha_k^{(f-1)}\}$ is equal to $\{s_0/t, ..., s_{f-1}/t\}$ where $\{s_0, ..., s_{f-1}\}$ is precisely equal to the coset $c_k\langle r \rangle$ in $H/\langle r \rangle$. Since $\{c_1, ..., c_g\}$ is a complete set of coset representatives of $H/\langle r \rangle$ and each element of H is in exactly one such coset, the product of Γ_p factors in (3.6) is precisely

$$\prod_{k=1}^{g} \prod_{i=0}^{f-1} \Gamma_p(\alpha_k^{(i)}) = \prod_{l=1}^{fg} \Gamma_p(\beta_l). \tag{3.7}$$

Now write $-\alpha_k = \sum_{j=0}^{\infty} \mu_{\alpha_k}^{(j)} p^j$ and set $a_k = (q-1)\alpha_k = \sum_{j=0}^{f-1} \mu_{\alpha_k}^{(j)} p^j$. Any $b_l \in H$ lies in precisely one coset $c_k\langle r\rangle$ and $\beta_l = \alpha_k^{(i)}$ for that value of k and precisely one i, $0 \le i \le f-1$; for these i, k we have $-\beta_l = \sum_{j=0}^{\infty} \mu_{\alpha_k}^{(i+j)} p^j$ and $n_{l,s} = \sum_{j=0}^{s-1} \mu_{\alpha_k}^{(i+j)} p^j$ for all $s \ge 0$. Therefore for any $s > 0$

$$\begin{aligned} \sum_{b_l \in c_k\langle r\rangle} n_{l,s} &= \sum_{i=0}^{f-1} \sum_{j=0}^{s-1} \mu_{\alpha_k}^{(i+j)} p^j \\ &= \sum_{j=0}^{s-1} p^j \sum_{i=0}^{f-1} \mu_{\alpha_k}^{(i+j)} = \sum_{j=0}^{s-1} p^j S(a_k) = \frac{p^s-1}{p-1} S(a_k). \end{aligned} \tag{3.8}$$

Taking $s = f$ in (3.8) gives

$$\sum_{b_l \in c_k\langle r\rangle} (q-1)\beta_l = \frac{q-1}{p-1} S(a_k) \tag{3.9}$$

and therefore

$$S = \sum_{k=1}^{g} S(a_k) = (p-1) \sum_{b_l \in H} \beta_l = (p-1)c \tag{3.10}$$

where c is as in (2.6). Then for any $s > 0$ we have

$$n_s = \sum_{b_l \in H} n_{l,s} = \sum_{k=1}^{g} \sum_{b_l \in c_k\langle r\rangle} n_{l,s} = \frac{p^s-1}{p-1} S = c(p^s-1), \tag{3.11}$$

so $n_s + c = cp^s \equiv 0 \pmod{p^s}$. Therefore

$$\begin{aligned} \prod_{k=1}^{g} g(\omega_f^{-c_k(q-1)/t}) &= (-p)^c \frac{\prod_{l=1}^{fg} \Gamma_p(\beta_l)}{\Gamma_p(0)} \\ &\equiv (-p)^c \frac{\prod_{l=1}^{fg} \Gamma_p(-n_{l,s})}{\Gamma_p(-n_s - c)} \pmod{p^{c+s}\mathbb{Z}_p}, \end{aligned} \tag{3.12}$$

and the stated congruences may now be obtained by application of Lemma 2.1, precisely as in Theorem 3.1.

We remark that in (2.6) we certainly have $c, d \le p$ when $p = tn + r$ with $n > 0$, so the second form of the congruences always holds in that case. We also recall that $-1 \notin H$ by definition, and therefore $-H = G \setminus H$. An identical argument produces the following congruence for the other product in (2.7).

THEOREM 3.3. *Let $p = tn + r$ be an odd prime and let f be the order of r in $(\mathbb{Z}/t\mathbb{Z})^\times$. With notations as in Section 2, write $-H = \{d_1, ..., d_{fg}\}$, set $\delta_l = d_l/t$, and define the nonnegative integer*

$m_{l,s} = p^s\delta_l^{(s)} - \delta_l$ *for* $1 \le l \le fg$ *and* $s \ge 0$. *Let* $m_s = \sum_{l=1}^{fg} m_{l,s}$ *and define* d *as in* (2.6). *Then for all* $s > 0$ *we have the congruence*

$$\frac{\binom{m_s + d}{m_{1,s}, \ldots, m_{fg,s}, d}}{\binom{m_{s-1} + d}{m_{1,s-1}, \ldots, m_{fg,s-1}, d}} \equiv \prod_{k=1}^{g} g(\omega_f^{c_k(q-1)/t}) \pmod{p^{d+s}\mathbb{Z}_p}.$$

If in addition we have $d \le p$ *then for all* $s > 0$ *we also have*

$$p \cdot \frac{\binom{m_s}{m_{1,s}, \ldots, m_{fg,s}}}{\binom{m_{s-1}}{m_{1,s-1}, \ldots, m_{fg,s-1}}} \equiv \prod_{k=1}^{g} g(\omega_f^{c_k(q-1)/t}) \pmod{p^{d+s}\mathbb{Z}_p}.$$

It will be observed that when r has order $f = \phi(t)/2$ in G we have $g = 1$ and the results of Theorems 3.2 and 3.3 are covered by Theorem 3.1. This is the case first considered in [9], [14].

4. Application to the Splitting of Rational Primes.

In this section we will relate our congruences to the splitting of rational primes following the work of Lee and Hahn [14], [15] and Hahn and Lee [9]. For this we consider odd primes p of the form $p = tn + r$, where p splits in $\mathbb{Q}(\sqrt{-t})$, and t is of one of the three forms

(1) $t = k > 3$ for a prime $k \equiv 3 \pmod 4$;

(2) $t = 4k$ for a prime $k \equiv 1 \pmod 4$;

(3) $t = 8k$ for any odd prime k.

For such values of t, we observe that $-t$ is a fundamental discriminant for which p splits in $\mathbb{Q}(\sqrt{-t})$ if and only if $r \in H$. We define the integers c and d by (2.6) and let $h = d - c$ denote the class number of $\mathbb{Q}(\sqrt{-t})$. All other notation is the same as in Theorems 3.2 and 3.3.

Theorem 4.1. *Suppose* $k > 3$ *is a prime,* $k \equiv 3 \pmod 4$, *and* $p = kn + r$ *is an odd prime which splits in* $\mathbb{Q}(\sqrt{-k})$. *Then* $4p^h = a^2 + kb^2$ *where*

$$a \equiv p^{-c}\left(\frac{\binom{n_s + c}{n_{1,s}, \ldots, n_{fg,s}, c}}{\binom{n_{s-1} + c}{n_{1,s-1}, \ldots, n_{fg,s-1}, c}} + \frac{\binom{m_s + d}{m_{1,s}, \ldots, m_{fg,s}, d}}{\binom{m_{s-1} + d}{m_{1,s-1}, \ldots, m_{fg,s-1}, d}}\right) \pmod{p^s\mathbb{Z}_p}$$

for all $s > 0$.

Proof. Under the stated hypotheses Hahn and Lee ([15], Theorem 3.1) showed that

$$\prod_{k=1}^{g} g(\omega_f^{-c_k(q-1)/t}) = p^c \left(\frac{a+b\sqrt{-k}}{2}\right) \tag{4.1}$$

and

$$\prod_{k=1}^{g} g(\omega_f^{c_k(q-1)/t}) = p^c \left(\frac{a-b\sqrt{-k}}{2}\right) \tag{4.2}$$

where $4p^h = a^2 + kb^2$. It follows from Theorems 3.2 and 3.3 above that

$$p^c \left(\frac{a+b\sqrt{-k}}{2}\right) \equiv \frac{\binom{n_s+c}{n_{1,s},\ldots,n_{fg,s},c}}{\binom{n_{s-1}+c}{n_{1,s-1},\ldots,n_{fg,s-1},c}} \pmod{p^{c+s}\mathbb{Z}_p} \tag{4.3}$$

and

$$p^c \left(\frac{a-b\sqrt{-k}}{2}\right) \equiv \frac{\binom{m_s+d}{m_{1,s},\ldots,m_{fg,s},d}}{\binom{m_{s-1}+d}{m_{1,s-1},\ldots,m_{fg,s-1},d}} \pmod{p^{d+s}\mathbb{Z}_p} \tag{4.4}$$

for all $s > 0$, yielding the stated result.

By the remark following Theorem 3.2 the statement of Theorem 4.1 applies also to the second form of the congruences of Theorems 3.2, 3.3 when $n > 0$. The next two theorems similarly follow from Theorems 3.2 and 3.3 and ([15], Theorems 4.1, 5.1).

THEOREM 4.2. *Suppose k is a prime, $k \equiv 1 \pmod 4$, and $p = 4kn + r$ is an odd prime which splits in $\mathbb{Q}(\sqrt{-k})$. Then $p^h = a^2 + kb^2$ where*

$$2a \equiv p^{-c}\left(\frac{\binom{n_s+c}{n_{1,s},\ldots,n_{fg,s},c}}{\binom{n_{s-1}+c}{n_{1,s-1},\ldots,n_{fg,s-1},c}} + \frac{\binom{m_s+d}{m_{1,s},\ldots,m_{fg,s},d}}{\binom{m_{s-1}+d}{m_{1,s-1},\ldots,m_{fg,s-1},d}}\right) \pmod{p^s\mathbb{Z}_p}$$

for all $s > 0$.

THEOREM 4.3. *Suppose k is an odd prime and $p = 8kn + r$ is an odd prime which splits in $\mathbb{Q}(\sqrt{-2k})$. Then $p^h = a^2 + 2kb^2$ where*

$$2a \equiv p^{-c}\left(\frac{\binom{n_s+c}{n_{1,s},\ldots,n_{fg,s},c}}{\binom{n_{s-1}+c}{n_{1,s-1},\ldots,n_{fg,s-1},c}} + \frac{\binom{m_s+d}{m_{1,s},\ldots,m_{fg,s},d}}{\binom{m_{s-1}+d}{m_{1,s-1},\ldots,m_{fg,s-1},d}}\right) \pmod{p^s\mathbb{Z}_p}$$

for all $s > 0$.

5. The case $t = 7$.

In this section we give an example to show how the tables of congruences for binomial coefficients modulo p in [15] may be extended to arbitrary powers of p, revealing their connection to differentials on formal group laws. M. Coster [5] gave several similar congruences in the case where $r = 1$ and $t = 2, 3, 4, 6$ using Jacobi sums over $\mathbb{F}_p$.

Theorem 5.1. *Define a sequence of integers* $\{a_N\}_{N=1}^{\infty}$ *by*

$$a_N = \begin{cases} \binom{3k}{k}, & \text{if } N = 7k+1, \\ -\binom{3k}{k}, & \text{if } N = 7k+2, \\ \binom{3k+1}{k}, & \text{if } N = 7k+4, \\ 0, & \text{otherwise.} \end{cases}$$

Suppose $p = 7n + r$ *is an odd prime with* $r \in H = \{1, 2, 4\}$ *and write* $4p = a^2 + 7b^2$ *for integers* a, b. *Then for any positive integers* m, s *with* $m \equiv 1, 2,$ *or* $4 \pmod 7$, *we have*

$$\frac{a_{mp^s}}{a_{mp^{s-1}}} \equiv \frac{a + b\sqrt{-7}}{2} \pmod{p^s \mathbb{Z}_p}.$$

Proof. If $r = 1$ then $f = 1$, $g = 3$ and $R = H$, and if $r = 2$ or 4 then $f = 3$ and $g = 1$. In either case by (4.1), (2.6) and (2.5) we have $c = 1$ and

$$p\left(\frac{a + b\sqrt{-7}}{2}\right) = \prod_{k=1}^{g} g(\omega_f^{-c_k(q-1)/7}) = (-p)\Gamma_p(\tfrac{1}{7})\Gamma_p(\tfrac{2}{7})\Gamma_p(\tfrac{4}{7}). \tag{5.1}$$

We now complete the proof in the case $p = 7n + 4$, the other cases being similar.

If $mp^s \equiv 4 \pmod 7$, write $mp^s = 7m_1 + 4$ so $m_1 = (mp^s - 4)/7$. In this case $m_1 = pk_1 + l_1$ with $k_1 = (mp^{s-1} - 1)/7$ and $l_1 = (p - 4)/7$. Set $m_2 = 2m_1 + 1 = (2mp^s - 1)/7$, so that $m_2 = pk_2 + l_2$ with $k_2 = 2k_1$ and $l_2 = 2l_1 + 1 = (2p - 1)/7$. We apply Lemma 2.1 with $\delta = \varepsilon = 0$ to get

$$\begin{aligned} \frac{a_{mp^s}}{a_{mp^{s-1}}} &= \frac{\binom{3m_1+1}{m_1}}{\binom{3k_1}{k_1}} \\ &= \frac{\Gamma_p(-m_1)\Gamma_p(1-2m_1)}{\Gamma_p(1-3m_1)} \equiv \frac{\Gamma_p(\frac{4}{7})\Gamma_p(\frac{1}{7})}{\Gamma_p(\frac{5}{7})} \pmod{p^s \mathbb{Z}_p}. \end{aligned} \tag{5.2}$$

For $x = 5/7$ we have $x' = 3/7$ and $\mu_x = (3p-5)/7 = 3n+1$ which is even, so that $\Gamma_p(5/7)\Gamma_p(2/7) = -1$ by (2.3). Therefore

$$\frac{a_{mp^s}}{a_{mp^{s-1}}} \equiv -\Gamma_p(\frac{1}{7})\Gamma_p(\frac{2}{7})\Gamma_p(\frac{4}{7}) \pmod{p^s\mathbb{Z}_p}, \tag{5.3}$$

and the stated congruence then follows from (5.1).

If $mp^s \equiv 1 \pmod 7$, write $mp^s = 7m_1 + 1$ so $m_1 = (mp^s - 1)/7$. In this case $m_1 = pk_1 + l_1$ with $k_1 = (mp^{s-1} - 2)/7$ and $l_1 = (2p-1)/7$. Set $m_2 = 2m_1 = (2mp^s - 2)/7$, so that $m_2 = pk_2 + l_2$ with $k_2 = 2k_1$ and $l_2 = 2l_1 = (4p-2)/7$. We again apply Lemma 2.1 with $\delta = \varepsilon = 0$ to get

$$\begin{aligned} \frac{a_{mp^s}}{a_{mp^{s-1}}} &= \frac{\binom{3m_1}{m_1}}{-\binom{3k_1}{k_1}} \\ &= -\frac{\Gamma_p(-m_1)\Gamma_p(-2m_1)}{\Gamma_p(-3m_1)} \equiv -\frac{\Gamma_p(\frac{1}{7})\Gamma_p(\frac{2}{7})}{\Gamma_p(\frac{3}{7})} \pmod{p^s\mathbb{Z}_p}. \end{aligned} \tag{5.4}$$

For $x = 3/7$ we have $x' = 6/7$ and $\mu_x = (6p-3)/7 = 6n+3$ which is odd, so that $\Gamma_p(3/7)\Gamma_p(4/7) = 1$ by (2.3). Therefore we again have

$$\frac{a_{mp^s}}{a_{mp^{s-1}}} \equiv -\Gamma_p(\frac{1}{7})\Gamma_p(\frac{2}{7})\Gamma_p(\frac{4}{7}) \pmod{p^s\mathbb{Z}_p}. \tag{5.5}$$

If $mp^s \equiv 2 \pmod 7$, write $mp^s = 7m_1 + 2$ so $m_1 = (mp^s - 2)/7$. In this case $m_1 = pk_1 + l_1$ with $k_1 = (mp^{s-1} - 4)/7$ and $l_1 = (4p-2)/7$. Set $m_2 = 2m_1 = (2mp^s - 4)/7$, so that $m_2 = pk_2 + l_2$ with $k_2 = 2k_1 + 1 = (2mp^{s-1} - 1)/7$ and $l_2 = 2l_1 - p = (p-4)/7$. We apply Lemma 2.1 with $\delta = \varepsilon = 0$ to get

$$\begin{aligned} \frac{a_{mp^s}}{a_{mp^{s-1}}} &= \frac{-\binom{3m_1}{m_1}}{\binom{3k_1+1}{k_1}} \\ &= -\frac{\Gamma_p(-m_1)\Gamma_p(-2m_1)}{\Gamma_p(-3m_1)} \equiv -\frac{\Gamma_p(\frac{2}{7})\Gamma_p(\frac{4}{7})}{\Gamma_p(\frac{6}{7})} \pmod{p^s\mathbb{Z}_p}. \end{aligned} \tag{5.6}$$

For $x = 6/7$ we have $x' = 5/7$ and $\mu_x = (5p-6)/7 = 5n+2$ which is odd, so that $\Gamma_p(6/7)\Gamma_p(1/7) = 1$ by (2.3). Therefore once again we have

$$\frac{a_{mp^s}}{a_{mp^{s-1}}} \equiv -\Gamma_p(\frac{1}{7})\Gamma_p(\frac{2}{7})\Gamma_p(\frac{4}{7}) \pmod{p^s\mathbb{Z}_p}. \tag{5.7}$$

The proofs for the cases $p = 7n + 1$ and $p = 7n + 2$ are entirely similar.

Table I of [15] may be obtained by taking $m = s = 1$ in this theorem. We observe that the sequence $\{a_N\}$ constructed in this theorem in fact arises as the sequence of expansion coefficients of the invariant differential on a formal group law over $\mathbb{Z}_p$ attached to the p-adic unit part of a product of Gauss sums, for any odd prime p of the form $p = 7n + r$ with $r \in \{1, 2, 4\}$.

COROLLARY 5.2. *Let $\{a_N\}$ be the sequence of integers described in Theorem 5.1. Then for any odd prime p of the form $p = 7n + r$ with $r \in \{1, 2, 4\}$ the formal power series*

$$\lambda(T) = \sum_{N=1}^{\infty} a_N \frac{T^N}{N} \in \mathbb{Q}[[T]]$$

is the logarithm of a one-dimensional formal group law over $\mathbb{Z}_p$; equivalently, the formal differential form

$$\omega = \sum_{N=1}^{\infty} a_N T^N \frac{dT}{T}$$

is the canonical invariant differential on this formal group law.

Proof. By Hazewinkel's functional equation lemma [10], since $a_1 = 1$ the assertion is equivalent to the existence of $H \in \mathbb{Z}_p$ such that

$$a_{mp^s} \equiv H \cdot a_{mp^{s-1}} \pmod{p^s \mathbb{Z}_p} \tag{5.8}$$

for all positive integers m and s (cf. [17], A8, A9). For $H = (a + b\sqrt{-7})/2$ the congruences (5.8) are trivial when $m \equiv 0, 3, 5, 6 \pmod 7$ and follow from Theorem 5.1 when $m \equiv 1, 2, 4 \pmod 7$, completing the proof.

The formal group law can be written as $F(X, Y) = \lambda^{-1}(\lambda(X) + \lambda(Y)) \in \mathbb{Q}[[X, Y]]$; it is a power series in two variables with rational coefficients whose denominators are not divisible by any odd prime p of the form $p = 7n + r$ with $r \in \{1, 2, 4\}$.

REFERENCES

1. A. ADLER, Eisenstein and the Jacobian varieties of Fermat curves, *Rocky Mountain J. Math.* **27.1** (1997), 1-60.
2. B. C. BERNDT, R. J. EVANS, AND K. S. WILLIAMS, "Gauss and Jacobi Sums", Wiley-Interscience, New York, 1998.

3. S. Chowla, B. Dwork, and R. J. Evans, On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$, *J. Number Theory* **24** (1986), 188-196.
4. H. Cohen, "A Course in Computational Algebraic Number Theory", Springer-Verlag, New York, 1995.
5. M. Coster, Generalisation of a congruence of Gauss, *J. Number Theory* **29** (1988), 300-310.
6. G. Eisenstein, Zur Theorie der quadratischen Zerfällung der Primzahlen $8n+3$, $7n+2$, und $7n+4$, *J. Reine Angew. Math.* **37** (1848), 97-126.
7. C. F. Gauss, Theoria Residuorum Biquadraticorum, Commentatio Prima (1828) [Werke, vol. II, 65-92].
8. B. Gross and N. Koblitz, Gauss sums and the p-adic Γ-function, *Ann. Math.* **109** (1979), 569-581.
9. S. Hahn and D. H. Lee, Some congruences for binomial coefficients, *in* "Class Field Theory - Its Centenary and Prospect", Adv. Studies in Pure Math., Vol. 30, Math. Soc. Japan, 2001.
10. M. Hazewinkel, "Formal Groups and Applications", Academic Press, New York, 1978.
11. R. Hudson and K. S. Williams, Binomial coefficients and Jacobi sums, *Trans. Amer. Math. Soc.* **281.2** (1984), 431-505.
12. C. G. J. Jacobi, De residuis cubics commentatio numerosa, *J. Reine Angew. Math.* **2** (1827), 66-69.
13. C. G. J. Jacobi, Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie, *J. Reine Angew. Math.* **30** (1846), 166-182.
14. D. H. Lee and S. Hahn, Some congruences for binomial coefficients, II, *Proc. Japan Acad. Ser. A.* **76.7** (2000), 104-107.
15. D. H. Lee and S. Hahn, Gauss sums and binomial coefficients, *J. Number Theory* **92** (2002), 257-271.
16. L. Stickelberger, Über eine Verallgemeinerung der Kreistheilung, *Math. Annalen* **37** (1890), 321-367.
17. J. Stienstra and F. Beukers, On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces, *Math. Annalen* **271** (1985), 269-304.
18. L. Washington, "Introduction to Cyclotomic Fields", Springer-Verlag, New York, 1982.
19. K. M. Yeung, On congruences for binomial coefficients, *J. Number Theory* **33** (1989), 1-17.
20. P. T. Young, On Jacobi sums, multinomial coefficients, and p-adic hypergeometric functions, *J. Number Theory* **52** (1995), 125-144.