Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 445–461

Some Congruences for Binomial Coefficients

Sang Geun Hahn and Dong Hoon Lee

Abstract.

Suppose that $p = tn + r$ is a prime and that h is the class number of the imaginary quadratic field, $\mathbb{Q}(\sqrt{-t})$. If $t \equiv 3 \pmod 4$ is a prime, just r is a quadratic residue modulo t and the order of r modulo t is $\frac{t-1}{2}$, then $4p^h$ can be written in the form $a^2 + tb^2$ for some integers a and b. And if $t = 4k$ where $k \equiv 1 \pmod 4$, $r \equiv 3 \pmod 4$, r is a quadratic non-residue modulo t and the order of r modulo t is $k - 1$, then $p^h = a^2 + kb^2$ for some integers a and b. Our result is that a or $2a$ is congruent modulo p to a product of certain binomial coefficients modulo sign. As an example, we give explicit formulas for $t = 11, 19, 20$ and 23.

§1. Introduction

Let p be a prime number throughout the paper. Gauss [1, 3, 4] proved that if $p = 4n + 1$ then $p = a^2 + b^2$ where $a \equiv 1 \pmod 4$ and

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

Jacobi [4, 6] proved that if $p = 3n + 1$ then $4p = a^2 + 27b^2$ where $a \equiv 1 \pmod 3$ and

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

Eisenstein [1, 2] proved several results. If $p = 8n + 3$ then $p = a^2 + 2b^2$ where $a \equiv (-1)^n \pmod 4$ and

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

Received September 14, 1998.

He also proved that if p is a prime of the form $p = 7n + 2$ or $7n + 4$ then $p = a^2 + 7b^2$ where $a \equiv p^2 \pmod 7$ and

$$2a \equiv \begin{cases} -\binom{3n}{n} \pmod p & \text{if } p = 7n + 2, \\ \binom{3n+1}{n} \pmod p & \text{if } p = 7n + 4. \end{cases}$$

In this paper we study similar problems for primes of the form $p = tn + r$.

§2. $t \equiv 3 \pmod 4$ is a prime

Since $t \equiv 3 \pmod 4$, the ring of integers of $\mathbb{Q}(\sqrt{-t})$ is $\mathbb{Z}[\frac{1+\sqrt{-t}}{2}]$ and $\mathbb{Q}(\zeta_t)$ is the extension field of $\mathbb{Q}(\sqrt{-t})$ with degree $\frac{\phi(t)}{2} = \frac{t-1}{2}$. Set $s = \frac{\phi(t)}{2}$. Let r be a quadratic residue modulo t such that $1 < r < t$ and the order of r modulo t is s. If s is a prime, then the order of a quadratic residue r modulo t such that $1 < r < t$ is s. Let $p = tn + r$ be a prime. By Dirichlet's theorem, there are infinitely many primes of this type since $(r, t) = 1$. Then

$$\left(\frac{-t}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{t}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{t-1}{2}\frac{p-1}{2}}\left(\frac{r}{t}\right) = 1$$

where $\left(\frac{\cdot}{\cdot}\right)$ is Legendre symbol. So p splits in $\mathbb{Q}(\sqrt{-t})$ as $p = \mathfrak{p}_1\mathfrak{p}_2$. Let $\tilde{\mathfrak{p}}_i$ be the prime ideal of $\mathbb{Q}(\zeta_t)$ over $\mathfrak{p}_i$. Since the order of r modulo t is s, so is the order of p. Hence the residue class degree of $\tilde{\mathfrak{p}}_i/p$ is s and $\mathfrak{p}_i$ is inert in $\mathbb{Q}(\zeta_t)/\mathbb{Q}(\sqrt{-t})$. Let $q = p^s$. If $\mathfrak{P}_i$ is a prime in $\mathbb{Q}(\zeta_{q-1})$ lying above $\tilde{\mathfrak{p}}_i$, then the residue class degree of $\mathfrak{P}_i/p$ is also s, hence we can identify $\mathbb{Z}[\zeta_{q-1}]/\mathfrak{P}_1$ with $\mathbb{F}_q$ where $\mathbb{F}_q$ is a finite field with q elements. Note that $\mathfrak{P}_i/p$ is unramified.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{q-1}) \arrow[d, dash] & \mathbb{Z}[\zeta_{q-1}] \arrow[d, dash] & \mathfrak{P}_1 \arrow[d, dash] & & \mathfrak{P}_2 \arrow[d, dash] \\
\mathbb{Q}(\zeta_t) \arrow[d, dash, "s"'] & \mathbb{Z}[\zeta_t] \arrow[d, dash] & \tilde{\mathfrak{p}}_1 \arrow[d, dash] & & \tilde{\mathfrak{p}}_2 \arrow[d, dash] \\
\mathbb{Q}(\sqrt{-t}) \arrow[d, dash, "2"'] & \mathbb{Z}[\frac{1+\sqrt{-t}}{2}] \arrow[d, dash] & \mathfrak{p}_1 \arrow[dr, dash] & & \mathfrak{p}_2 \arrow[dl, dash] \\
\mathbb{Q} & \mathbb{Z} & & p &
\end{tikzcd}$$

2.1. Gauss Sums

The unit group of the finite field $\mathbb{F}_q^\times$ can be identified with the $(q-1)$-st roots of unity via Teichmüller character ω:

$$\omega = \omega_{\mathfrak{P}_1} : \mathbb{F}_q^\times \longrightarrow \langle \zeta_{q-1} \rangle$$

satisfying

$$\omega(a) \equiv a \pmod{\mathfrak{P}_1} \text{ for all } a \in \mathbb{F}_q^\times$$

where ζ_{q-1} is the primitive $(q-1)$-st root of unity. Let χ be a multiplicative character such that

$$\begin{aligned} \chi : \mathbb{F}_q^\times &\longrightarrow \langle \zeta_t \rangle \\ a &\longmapsto \omega(a)^{\frac{q-1}{t}} \end{aligned}$$

where ζ_t is the primitive t-th root of unity. Note that $t|(q-1)$. Define the Gauss sum as follows:

$$g(\chi) := -\sum_{a \in \mathbb{F}_q} \chi(a) \zeta_p^{tr(a)}$$

where $tr : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ is the trace map and ζ_p is the primitive p-th root of unity. Note that $g(\chi) \in \mathbb{Q}(\zeta_{tp})$ since $\chi(a) \in \mathbb{Q}(\zeta_t)$.

Definition 2.1.1 (Adler [1]).

$$\Gamma_\nu := \sum_{a \in \mathbb{F}_q^\times,\ tr(a)=1} \chi^\nu(a)$$

Lemma 2.1.2 (Adler).

$$g(\chi^\nu) = p\Gamma_\nu \textit{ for } \chi = \omega^{\frac{q-1}{t}}$$

Proof.

$$
\begin{aligned}
&g(\chi^\nu)\\
=&-\Big(\sum_{\substack{a\in\mathbb{F}_q^\times\\ tr(a)=0}}\chi^\nu(a)+\zeta_p\sum_{\substack{a\in\mathbb{F}_q^\times\\ tr(a)=1}}\chi^\nu(a)+\cdots+\zeta_p^{p-1}\sum_{\substack{a\in\mathbb{F}_q^\times\\ tr(a)=p-1}}\chi^\nu(a)\Big)\\
=&(1-\zeta_p)\Big(\sum_{\substack{a\in\mathbb{F}_q^\times\\ tr(a)=1}}\chi^\nu(a)\Big)+\cdots+(1-\zeta_p^{p-1})\Big(\sum_{\substack{a\in\mathbb{F}_q^\times\\ tr(a)=p-1}}\chi^\nu(a)\Big)\\
&\left(\text{since } \chi^\nu \text{ is a non-trivial character, } \sum_{a\in\mathbb{F}_q^\times}\chi^\nu(a)=0\right)\\
=&(1-\zeta_p)\Big(\sum_{\substack{a\in\mathbb{F}_q^\times\\ tr(a)=1}}\chi^\nu(a)\Big)+\cdots+(1-\zeta_p^{p-1})\Big(\sum_{\substack{a\in\mathbb{F}_q^\times\\ tr(a)=1}}\chi^\nu((p-1)a)\Big)\\
=&((1-\zeta_p)+(1-\zeta_p^2)\chi^\nu(2)+\cdots+(1-\zeta_p^{p-1})\chi^\nu(p-1))\Gamma_\nu.
\end{aligned}
$$

For $a\in\mathbb{F}_p^\times$, $a^{\frac{q-1}{t}}=(a^{p-1})^{\frac{q-1}{t(p-1)}}=1$ because $t,(p-1)|(q-1)$ and $(t,p-1)=1$. Hence

$$\chi^\nu(a)=\omega(a)^{\frac{q-1}{t}\nu}=\omega(1)^\nu=1.$$

Therefore

$$
\begin{aligned}
g(\chi^\nu) &= \{(p-1)-(\zeta_p+\zeta_p^2+\cdots+\zeta_p^{p-1})\}\Gamma_\nu\\
&= p\Gamma_\nu.
\end{aligned}
$$

□

Definition 2.1.3 ([1]).

$$\phi(x):=\sum_{j=0}^{t-1}c_jx^j$$

where $c_j=\#\{a\in\mathbb{F}_q^\times \mid tr(a)=1,\quad \chi(a)=\zeta_t^j\}$.

Then $\phi(\zeta_t^\nu)=\sum_{j=0}^{t-1}c_j(\zeta_t^j)^\nu=\sum_{\substack{a\in\mathbb{F}_q^\times\\ tr(a)=1}}\chi^\nu(a)=\Gamma_\nu$. We know that

$$tr(a)=a+a^p+a^{p^2}+\cdots+a^{p^{s-1}}=tr(a^p).$$

Hence

$$\begin{aligned} c_j &= \#\{a \in \mathbb{F}_q^\times \mid tr(a) = 1, \quad \chi(a) = \zeta_t^j\} \\ &= \#\{a \in \mathbb{F}_q^\times \mid tr(a^p) = 1, \quad \chi(a^p) = \zeta_t^{pj}\} \\ &= \#\{b \in \mathbb{F}_q^\times \mid tr(b) = 1, \quad \chi(b) = \zeta_t^{pj}\} \\ &= c_{pj}. \end{aligned}$$

Since c_j is determined by $j \pmod t$ and $p \equiv r \pmod t$, $c_j = c_{pj} = c_{rj}$.

Lemma 2.1.4.

$$g(\chi^\nu) \in \mathbb{Q}(\sqrt{-t})$$

Proof. The Galois group $Gal(\mathbb{Q}(\zeta_t)/\mathbb{Q}(\sqrt{-t}))$ is cyclic of order s generated by

$$\begin{aligned} \tau : \mathbb{Q}(\zeta_t) &\longrightarrow \mathbb{Q}(\zeta_t) \\ \zeta_t &\longmapsto \zeta_t^r \end{aligned}$$

Hence

$$\begin{aligned} \tau(\Gamma_\nu) &= \tau\Big(\sum_{j=0}^{t-1} c_j (\zeta_t^j)^\nu\Big) \\ &= \sum_{j=0}^{t-1} c_j (\zeta_t^{rj})^\nu \\ &= \sum_{j=0}^{t-1} c_{rj} (\zeta_t^{rj})^\nu \\ &= \Gamma_\nu. \end{aligned}$$

So $\Gamma_\nu \in \mathbb{Q}(\sqrt{-t})$. By Lemma 2.1.2, the above lemma is proved. □

Definition 2.1.5 (Washington [10]).

$$\theta := \sum_{b=1}^{t-1} \frac{b}{t} \sigma_b^{-1} \in \mathbb{Q}[Gal(\mathbb{Q}(\zeta_t)/\mathbb{Q})]$$

where $\sigma_b : \mathbb{Q}(\zeta_t) \longrightarrow \mathbb{Q}(\zeta_t)$ *such that* $\sigma_b(\zeta_t) = \zeta_t^b$.

θ is called the Stickelberger element for $\mathbb{Q}(\zeta_t)/\mathbb{Q}$. Since $\chi = \omega^{\frac{q-1}{t}}$

$$\Big(g(\chi^{-1})^t\Big) = \tilde{\mathfrak{p}}_1^{t\theta} = \tilde{\mathfrak{p}}_1^{\sum_{b=1}^{t-1} b\sigma_b^{-1}}$$

by Stickelberger's theorem.
$Gal(\mathbb{Q}(\zeta_t)/\mathbb{Q}(\sqrt{-t})) = \{\sigma_b | b \text{ is a quadratic residue modulo } t\}$ fixes $\tilde{\mathfrak{p}}_1$, and all the other σ_bs send $\tilde{\mathfrak{p}}_1$ to $\tilde{\mathfrak{p}}_2$. So

$$\left(g(\chi^{-1})^t\right) = \tilde{\mathfrak{p}}_1^{\sum_{(\frac{b}{t})=1} b} \tilde{\mathfrak{p}}_2^{\sum_{(\frac{b}{t})=-1} b}.$$

Let $\sum_{(\frac{b}{t})=1} b = \alpha t$, $\sum_{(\frac{b}{t})=-1} b = \beta t$ for some integers $\alpha, \beta \geq 1$. Then

$$\left(g(\chi^{-1})\right) = \tilde{\mathfrak{p}}_1^{\alpha} \tilde{\mathfrak{p}}_2^{\beta} \subset \mathbb{Z}[\zeta_t].$$

Note that $\left(g(\chi)\right) = \tilde{\mathfrak{p}}_1^{\beta} \tilde{\mathfrak{p}}_2^{\alpha}$ and $\tilde{\mathfrak{p}}_1 \tilde{\mathfrak{p}}_2 = (p)$ in $\mathbb{Q}(\zeta_t)$.

Lemma 2.1.6.

$$\begin{aligned} \left(g(\chi)\right) &= \mathfrak{p}_1^{\beta} \mathfrak{p}_2^{\alpha} \\ \left(g(\chi^{-1})\right) &= \mathfrak{p}_1^{\alpha} \mathfrak{p}_2^{\beta} \end{aligned}$$

as ideals in $\mathbb{Z}[\frac{1+\sqrt{-t}}{2}]$.

Proof. $g(\chi) \in \mathbb{Q}(\sqrt{-t})$ by Lemma 2.1.4 and $\tilde{\mathfrak{p}}_i \cap \mathbb{Q}(\sqrt{-t}) = \mathfrak{p}_i$. So we are done. □

Consider the analytic class number formula

$$\frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|d|}} = \prod_{\substack{\psi \in X \\ \chi \neq id}} L(1, \psi)$$

for abelian extensions. We know that if $\psi(-1) = -1$ then

$$L(1, \psi) = \pi i \frac{\tau(\psi)}{f} \frac{1}{f} \sum_{a=1}^{f-1} \bar{\psi}(a) a$$

where f is the conductor of ψ and $\tau(\psi) = \sum_{a=1}^{f} \psi(a) e^{2\pi i/f}$ is a Gauss sum.
Apply these formulas to $\mathbb{Q}(\sqrt{-t})$. Then $r_1 = 0, r_2 = 1, R = 1, w = 2, |d| = t$, and $\psi = (\frac{\cdot}{t})$. Hence $f = t$ and $|\tau(\psi)| = \sqrt{t}$. So

$$\frac{2\pi h}{2\sqrt{t}} = \frac{\pi h}{\sqrt{t}} = L(1, \left(\frac{\cdot}{t}\right)).$$

By taking the absolute value

$$\begin{aligned} h &= \frac{\sqrt{t}}{\pi}\Big|L(1,\Big(\frac{\cdot}{t}\Big))\Big| = \frac{\sqrt{t}}{\pi}\Big|\pi i\frac{\sqrt{t}}{t}\frac{1}{t}\sum_{a=1}^{t-1}\overline{\Big(\frac{a}{t}\Big)a}\Big| \\ &= \frac{1}{t}\Big|\sum_{b=1}^{t-1}\Big(\frac{b}{t}\Big)b\Big| \\ &= \frac{1}{t}\Big|\sum_{(\frac{b}{t})=1} b - \sum_{(\frac{b}{t})=-1} b\Big| \\ &= \frac{1}{t}\Big|\alpha t - \beta t\Big| = \Big|\alpha - \beta\Big|. \end{aligned}$$

2.2. p-adic Gamma Function

Definition 2.2.1 (Lang [7]).

$$\Gamma_p(z) := \lim_{m\to z}(-1)^m \prod_{\substack{0<j<m \\ (p,j)=1}} j$$

where m approaches z p-adically through positive integers.

Definition 2.2.2 ([10]). *If $0 \le d \le q-1$ and $d = d_0 + d_1p + \cdots + d_{s-1}p^{s-1}$ such that $0 \le d_j < p$, define*

$$s(d) := \sum_{j=0}^{s-1} d_j.$$

Γ_p is called p-adic Gamma function. Note that if $\tilde{\mathfrak{P}}_1$ is a prime in $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ lying above $\mathfrak{P}_1$ then

$$s(d) = v_{\tilde{\mathfrak{P}}_1}(g(\omega^{-d}))$$

where $v_{\tilde{\mathfrak{P}}_1}$ is $\tilde{\mathfrak{P}}_1$-adic valuation.

Let Π be a $(p-1)$-st root of $-p$. Then Gross-Koblitz formula is

$$g(\omega^d) = (-p)^s \Pi^{-s(d)} \prod_{j=0}^{s-1} \Gamma_p\Big(1 - \Big\langle \frac{p^j d}{q-1} \Big\rangle\Big).$$

Lemma 2.2.3. *If* $d = \frac{q-1}{t}(t-1) = d_0 + d_1 p + \cdots + d_{s-1}p^{s-1}$ *and* $d' = \frac{q-1}{t} = d'_0 + d'_1 p + \cdots + d'_{s-1}p^{s-1}$, *then*

$$\begin{aligned} g(\chi^{-1}) &= (-p)^{\alpha} \prod_{j=0}^{s-1} \Gamma_p\Big(1 - \Big\langle \frac{p^j d}{q-1} \Big\rangle\Big), \\ g(\chi) &= (-p)^{\beta} \prod_{j=0}^{s-1} \Gamma_p\Big(1 - \Big\langle \frac{p^j d'}{q-1} \Big\rangle\Big). \end{aligned}$$

Proof. It is sufficient to show that $s(d) = (p-1)\beta$ and $s(d') = (p-1)\alpha$.

$$s(d) = v_{\tilde{\mathfrak{P}}_1}(g(\omega^{-d})) = v_{\tilde{\mathfrak{P}}_1}(g(\chi)).$$

Since $g(\chi) \in \mathbb{Q}(\sqrt{-t}), \mathfrak{P}_1 = \tilde{\mathfrak{P}}_1^{p-1}$ and $\mathfrak{P}_1/\mathfrak{p}_1$ is unramified, $v_{\tilde{\mathfrak{P}}_1} = (p-1)v_{\mathfrak{P}_1} = (p-1)v_{\mathfrak{p}_1}$. So by Lemma 2.1.5

$$s(d) = (p-1)v_{\mathfrak{p}_1}(g(\chi)) = (p-1)\beta.$$

Similary $s(d') = (p-1)\alpha$. So we are done. □

2.3. Main Result

Theorem 2.3.1. *Suppose that* $t \equiv 3 \pmod 4$ *is a prime and that* $r > 1$ *is a quadratic residue modulo* t *and its order is* $s = \frac{\phi(t)}{2} = \frac{t-1}{2}$. *Let* h *be the class number of* $\mathbb{Q}(\sqrt{-t})$ *and* $p = tn + r$ *be a prime. Let* $p = \mathfrak{p}_1\mathfrak{p}_2$ *in* $\mathbb{Z}[\frac{1+\sqrt{-t}}{2}]$, $\mathfrak{p}_1^h = \left(\frac{a+b\sqrt{-t}}{2}\right)$, $\sum_{(\frac{b}{t})=1} b = \alpha t$, $\sum_{(\frac{b}{t})=-1} b = \beta t$, $d = (\frac{q-1}{t})(t-1) = \sum_{j=0}^{s-1} d_j p^j$ *and* $d' = (\frac{q-1}{t}) = \sum_{j=0}^{s-1} d'_j p^j$ *as in the previous section. Then*

1. $4p^h = a^2 + tb^2$,
2.

$$a \equiv \begin{cases} \pm \prod_{j=0}^{s-1} (d_j)! \pmod p & \text{if } \alpha < \beta, \\ \pm \prod_{j=0}^{s-1} (d'_j)! \pmod p & \text{if } \beta < \alpha. \end{cases}$$

In particular, if $\mathfrak{p}_1$ *is principal ideal,* $\mathfrak{p}_1 = \left(\frac{A+B\sqrt{-t}}{2}\right)$, *then* $4p = A^2 + tB^2$ *and* $A^h \equiv \pm a \pmod p$.

Remark. Note that $h = |\alpha - \beta|$, and a and b are unique up to sign. Since $s(d)$ and $s(d')$ are multiples of $(p-1)$, $\prod(d_i)!$ and $\prod(d'_i)!$

can be expressed as some products of binomial coefficients by Wilson's Theorem.

Proof. The first statement is trivial.

For the second, we will prove only $\alpha < \beta$ case because the other case is done in a similar manner. By Lemma 2.1.6 and Gross-Koblitz formula,

$$\begin{aligned} \left(g(\chi^{-1})\right) &= \mathfrak{p}_1^{\alpha}\mathfrak{p}_2^{\beta} = p^{\alpha}\mathfrak{p}_2^{h} \\ g(\chi^{-1}) &= (-p)^{\alpha}\prod_{j=0}^{s-1}\Gamma_p\Big(1-\Big\langle\frac{p^j d}{q-1}\Big\rangle\Big). \end{aligned}$$

Hence

$$\frac{a-b\sqrt{-t}}{2} = \pm\prod_{j=0}^{s-1}\Gamma_p\Big(1-\Big\langle\frac{p^j d}{q-1}\Big\rangle\Big)$$

$$\frac{a+b\sqrt{-t}}{2}+\frac{a-b\sqrt{-t}}{2} \equiv \pm\prod_{j=0}^{s-1}\Gamma_p\Big(1-\Big\langle\frac{p^j d}{q-1}\Big\rangle\Big) \pmod{\mathfrak{p}_1}$$

$$a \equiv \pm\prod_{j=0}^{s-1}\Gamma_p\Big(1-\Big\langle\frac{p^j d}{q-1}\Big\rangle\Big) \pmod{p}.$$

Since

$$\Gamma_p\Big(1-\Big\langle\frac{p^{s-j} d}{q-1}\Big\rangle\Big) \equiv (-1)^{1+d_j}(d_j)! \pmod{p},$$

$$a \equiv \pm\prod_{j=0}^{s-1}(d_j)! \pmod{p}.$$

If $\mathfrak{p}_i$ is principal, then

$$\mathfrak{p}_1^h = \left(\frac{A+B\sqrt{-t}}{2}\right)^h = \left(\frac{a+b\sqrt{-t}}{2}\right)$$

as ideals. So

$$\left(\frac{A+B\sqrt{-t}}{2}\right)^h = \pm\left(\frac{a+b\sqrt{-t}}{2}\right).$$

Since $\dfrac{B\sqrt{-t}}{2} \equiv \dfrac{A}{2} \pmod{\mathfrak{p}_2}$ and $\dfrac{b\sqrt{-t}}{2} \equiv \dfrac{a}{2} \pmod{\mathfrak{p}_2}$, we have $A^h \equiv \pm a \pmod{p}$. $\square$

Example 2.3.2. Let $t = 7$, then $s = 3$, $\alpha = 1$, $\beta = 2$ so $h(\mathbb{Q}(\sqrt{-7})) = 1$. Since $h = 1$ if $4p = a^2 + 7b^2$ then a and b are unique up to sign. Let p be a prime of the form $7n+2$ or $7n+4$ and $d = 6(p^3 - 1)/7$. Then

$$d = \begin{cases} 3n + (5n+1)p + (6n+1)p^2 & \text{if } p = 7n+2, \\ (5n+2) + (3n+1)p + (6n+3)p^2 & \text{if } p = 7n+4. \end{cases}$$

By Theorem 2.3.1, if $4p = a^2 + 7b^2$, then

$$a \equiv \begin{cases} \pm(3n)!(5n+1)!(6n+1)! \pmod{p} & \text{if } p = 7n+2, \\ \pm(5n+2)!(3n+1)!(6n+3)! \pmod{p} & \text{if } p = 7n+4. \end{cases}$$

By Wilson's theorem, if p is a prime and $p - 1 = x + y$, then $x!y! \equiv (-1)^{y+1} \pmod{p}$. So we get the Eisenstein's result.

$$a \equiv \begin{cases} \pm(3n)! \cdot \dfrac{1}{(2n)!} \cdot \dfrac{1}{(n)!} \equiv \pm\dbinom{3n}{n} \pmod{p} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } p = 7n+2, \\ \pm\dfrac{1}{(2n+1)!} \cdot (3n+1)! \cdot \dfrac{1}{(n)!} \equiv \pm\dbinom{3n+1}{n} \pmod{p} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } p = 7n+4. \end{cases}$$

Since $a \leq 2\sqrt{p} < p/2$, the sign can be uniquely determined.

Example 2.3.3. Let $t = 11$, then $s = 5$, $\alpha = 2$, $\beta = 3$, and so $h(\mathbb{Q}(\sqrt{-11})) = 1$. Jacobi[4,5] showed that if $p = 11n + 1$ is a prime and $4p = a^2 + 11b^2$ where $a \equiv 2 \pmod{11}$ then

$$\begin{aligned} a &\equiv \frac{1}{(n)!(3n)!(4n)!(5n)!(9n)!} \pmod{p} \\ &\equiv \binom{3n}{n}\binom{6n}{3n}\binom{4n}{2n}^{-1} \pmod{p}. \end{aligned}$$

Suppose that $p = 11n + 5$ is a prime.

$$d = \frac{10(p^5 - 1)}{11} = 2n + (7n+3)p + (8n+3)p^2 + (6n+2)p^3 + (10n+4)p^4.$$

By Theorem 2.3.1, if $4p = a^2 + 11b^2$ then

$$\begin{aligned} a &\equiv \pm(2n)!(7n+3)!(8n+3)!(6n+2)!(10n+4)! \pmod{p} \\ &\equiv \pm\binom{3n+1}{n}\binom{6n+2}{3n+1}\binom{4n+1}{2n}^{-1} \pmod{p}. \end{aligned}$$

Since $a \leq 2\sqrt{p} < p/2$, the sign can be uniquely determined. In a similar manner, we can get the following corollary.

Corollary 2.3.4. *Let $p = 11n + r$ be a prime and $4p = a^2 + 11b^2$ where r is a quadratic residue modulo 11. Then*

$$a \equiv \begin{cases} \pm\binom{3n+1}{n}\binom{6n+1}{3n}\binom{4n+1}{2n}^{-1} \pmod p & \text{if } r = 3, \\ \pm\binom{3n+1}{n}\binom{6n+2}{3n+1}\binom{4n+1}{2n}^{-1} \pmod p & \text{if } r = 4 \text{ or } 5, \\ \pm\binom{3n+2}{n}\binom{6n+4}{3n+2}\binom{4n+3}{2n+1}^{-1} \pmod p & \text{if } r = 9. \end{cases}$$

Example 2.3.5. Let $t = 19$, then $s = 9$, $\alpha = 4$, $\beta = 5$, and so $h(\mathbb{Q}(\sqrt{-19})) = 1$. Since s is not a prime, the order of a quadratic residue is not always $s(= 9)$. Suppose $p = 19n + 4$ is a prime. Then

$$\begin{aligned} d &= (14n+2) + (13n+2)p + (8n+1)p^2 + (2n)p^3 + (10n+2)p^4 \\ &\quad +(12n+2)p^5 + (3n)p^6 + (15n+3)p^7 + (18n+3)p^8. \end{aligned}$$

If $4p = a^2 + 19b^2$, then by Theorem 2.3.1 and Wilson's theorem,

$$a \equiv \pm\binom{6n+1}{n}\binom{10n+1}{4n}\binom{10n+2}{3n+1}\binom{6n+1}{3n}^{-1}\binom{10n+1}{2n}^{-1} \pmod p.$$

Similarly we get the following corollary.

Corollary 2.3.6. *Let $p = 19n + r$ be a prime where r is a quadratic residue and its order is 9. If $4p = a^2 + 19b^2$, then a is congruent modulo p to a product of binomial coefficients modulo sign.*

1. $a \equiv \pm\binom{6n+1}{n}\binom{10n+1}{4n}\binom{10n+2}{3n+1}\binom{6n+1}{3n}^{-1}\binom{10n+1}{2n}^{-1}$
   if $r = 4$;
2. $a \equiv \pm\binom{6n+1}{n}\binom{10n+2}{4n+1}\binom{10n+2}{3n+1}\binom{6n+1}{3n}^{-1}\binom{10n+2}{2n}^{-1}$
   if $r = 5$;
3. $a \equiv \pm\binom{6n+1}{n}\binom{10n+2}{4n+1}\binom{10n+3}{3n+1}\binom{6n+1}{3n}^{-1}\binom{10n+2}{2n}^{-1}$
   if $r = 6$;
4. $a \equiv \pm\binom{3n+1}{n}\binom{10n+4}{5n+2}\binom{13n+5}{6n+2}\binom{4n+1}{2n}^{-1}\binom{13n+5}{5n+2}^{-1}$
   if $r = 9$;

5. $a \equiv \pm \binom{3n+2}{n}\binom{10n+8}{5n+4}\binom{13n+10}{6n+5}\binom{4n+3}{2n+1}^{-1}\binom{13n+10}{5n+4}^{-1}$
if $r = 16$;
6. $a \equiv \pm \binom{3n+2}{n}\binom{10n+8}{5n+4}\binom{13n+11}{6n+5}\binom{4n+3}{2n+1}^{-1}\binom{13n+11}{5n+4}^{-1}$
if $r = 17$.

Example 2.3.7. Suppose $p = 23n+4$ is a prime. Then $h(\mathbb{Q}(\sqrt{-23})) = 3$ and

$$\begin{aligned} d = {} & (17n+2) + (10n+1)p + (14n+2)p^2 + (15n+2)p^3 + (21n+3)p^4 \\ & + (11n+1)p^5 + (20n+3)p^6 + (5n)p^7 + (7n+1)p^8 + (19n+3)p^9 \\ & + (22n+3)p^{10}. \end{aligned}$$

If $4p^3 = a^2+23b^2$ for $p \not| a$, then by Theorem 2.3.1 and Wilson's theorem,

$$a \equiv \pm \binom{4n}{n}\binom{10n+1}{4n}\binom{11n+1}{2n}\binom{12n+1}{4n}\binom{12n+1}{5n}^{-1} \pmod p.$$

If $\mathfrak{p}_i$ is principal, then $4p$ can be written in the form $A^2 + 23B^2$. For example, if $p = 211$, then $4p = 4^2 + 23 \cdot 6^2$. So we can verify Theorem 2.3.1 that $4p^3 = 2468^2+23\cdot 1170^2$ and $4^2 \equiv -(2468) \pmod p$. Note that if $t \not\equiv 3 \pmod 8$ then a and b are even. Similarly we get the following corollary.

Corollary 2.3.8. *Let $p = 23n + r$ be a prime and $4p^3 = a^2 + 23b^2$ for $p \not| a$ where r is a quadratic residue modulo 23. Then a is congruent modulo p to a product of binomial coefficients modulo sign.*

1. $a \equiv \pm \binom{4n}{n}\binom{10n}{4n}\binom{11n}{2n}\binom{12n}{4n}\binom{12n}{5n}^{-1}$
if $r = 2$;
2. $a \equiv \pm \binom{5n}{2n}\binom{10n+1}{n}\binom{10n}{4n}\binom{11n+1}{3n}\binom{10n}{3n}^{-1}$
if $r = 3$;
3. $a \equiv \pm \binom{4n}{n}\binom{10n+1}{4n}\binom{11n+1}{2n}\binom{12n+1}{4n}\binom{12n+1}{5n}^{-1}$
if $r = 4$;
4. $a \equiv \pm \binom{4n}{n}\binom{10n+2}{4n+1}\binom{11n+2}{2n}\binom{12n+2}{4n}\binom{12n+2}{5n+1}^{-1}$
if $r = 6$;
5. $a \equiv \pm \binom{4n+1}{n}\binom{10n+3}{4n+1}\binom{11n+3}{2n}\binom{12n+3}{4n+1}\binom{12n+3}{5n+1}^{-1}$
if $r = 8$;

6. $a \equiv \pm \binom{5n+1}{2n}\binom{10n+3}{n}\binom{10n+3}{4n+1}\binom{11n+4}{3n+1}\binom{10n+3}{3n+1}^{-1}$
   if $r = 9$;
7. $a \equiv \pm \binom{4n+1}{n}\binom{10n+5}{4n+2}\binom{11n+5}{2n+1}\binom{12n+5}{4n+1}\binom{12n+5}{5n+2}^{-1}$
   if $r = 12$;
8. $a \equiv \pm \binom{4n+1}{n}\binom{10n+5}{4n+2}\binom{11n+6}{2n+1}\binom{12n+5}{4n+1}\binom{12n+5}{5n+2}^{-1}$
   if $r = 13$;
9. $a \equiv \pm \binom{4n+2}{n}\binom{10n+6}{4n+2}\binom{11n+7}{2n+1}\binom{12n+7}{4n+2}\binom{12n+7}{5n+3}^{-1}$
   if $r = 16$;
10. $a \equiv \pm \binom{4n+2}{n}\binom{10n+7}{4n+3}\binom{11n+8}{2n+1}\binom{12n+8}{4n+2}\binom{12n+8}{5n+3}^{-1}$
   if $r = 18$.

§3. $t = 4k$ for a prime $k \equiv 1 \pmod 4$

Suppose $p = 4kn + r$ is a prime where $k \equiv 1 \pmod 4$ is a prime and $r \equiv 3 \pmod 4$ is a quadratic non-residue modulo k, that is $\left(\frac{r}{k}\right) = -1$. Then the ring of integers of $\mathbb{Q}(\sqrt{-k})$ is $\mathbb{Z}[\sqrt{-k}]$ and

$$\left(\frac{-k}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{k}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{k-1}{2}\frac{p-1}{2}}\left(\frac{r}{k}\right) = 1.$$

So p splits in $\mathbb{Q}(\sqrt{-k})$ as $p = \mathfrak{p}_1\mathfrak{p}_2$. Suppose the order of r modulo t is $k-1$. Then $\mathfrak{p}_i$ is inert in $\mathbb{Q}(\zeta_t)/\mathbb{Q}(\sqrt{-k})$. Let $\tilde{\mathfrak{p}}_i$ be the prime ideal of $\mathbb{Q}(\zeta_t)$ over $\mathfrak{p}_i$ and $q = p^{k-1}$. If $\mathfrak{P}_i$ is a prime in $\mathbb{Q}(\zeta_{q-1})$ lying above $\tilde{\mathfrak{p}}_i$, then the residue class degree of $\mathfrak{P}_i$ is $k-1$; hence we can identify $\mathbb{Z}[\zeta_{q-1}]/\mathfrak{P}_1$ with $\mathbb{F}_q$. Note that $\mathfrak{P}_i/p$ is unramified.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{q-1}) \arrow[d, dash] & \mathbb{Z}[\zeta_{q-1}] \arrow[d, dash] & \mathfrak{P}_1 \arrow[d, dash] & & \mathfrak{P}_2 \arrow[d, dash] \\
\mathbb{Q}(\zeta_t) \arrow[d, dash] \arrow[d, bend right, dash, "k-1"'] & \mathbb{Z}[\zeta_t] \arrow[d, dash] & \tilde{\mathfrak{p}}_1 \arrow[d, dash] & & \tilde{\mathfrak{p}}_2 \arrow[d, dash] \\
\mathbb{Q}(\sqrt{-k}) \arrow[d, dash] \arrow[d, bend right, dash, "2"'] & \mathbb{Z}[\sqrt{-k}] \arrow[d, dash] & \mathfrak{p}_1 \arrow[dr, dash] & & \mathfrak{p}_2 \arrow[dl, dash] \\
\mathbb{Q} & \mathbb{Z} & & p &
\end{tikzcd}$$

3.1. Gauss Sums and p-adic Gamma Functions

Let χ be a multiplicative character such that

$$\begin{array}{rcl} \chi : \mathbb{F}_q^\times & \longrightarrow & \langle \zeta_t \rangle \\ a & \longmapsto & \omega(a)^{\frac{q-1}{t}} \end{array}$$

where ω is the Teichmüller character. $g(\chi)$, Γ_ν, $\phi(x)$ and Γ_p are defined as in the previous section.

Lemma 3.1.1.

$$g(\chi^\nu) = p\Gamma_\nu \textit{ for } \chi = \omega^{\frac{q-1}{t}}$$

Proof. It is sufficient to show that for $a \in \mathbb{F}_p^\times$, $a^{\frac{q-1}{t}} = 1$ as in the Lemma 2.1.2.

We will show that $4k(p-1)|(q-1)$. Since $r \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd. So $8, k$ and $\frac{p-1}{2}$ are relatively prime. Clearly $k|(q-1)$ and $\frac{p-1}{2}|(q-1)$.

$$\begin{aligned} q-1 &= (4kn+r)^{k-1} - 1 \\ &= \sum_{i=0}^{k-1} \binom{k-1}{i} (4kn)^i r^{k-1-i} - 1. \end{aligned}$$

If $i \geq 2$, then $8|(4kn)^i$. If $i = 1$, then $2|\binom{k-1}{1} = k-1$ and $4|4kn$, and hence $8|\binom{k-1}{1}(4kn)$. Since $r \equiv 3 \pmod 4$, $r^2 \equiv 1 \pmod 8$, and hence $(r^2)^{\frac{k-1}{2}} \equiv 1 \pmod 8$. So if $i = 0$, then $8|r^{k-1} - 1$. Thus we showed $8|(q-1)$, and hence $4k(p-1)|(q-1)$. So we are done. □

The Galois group $Gal(\mathbb{Q}(\zeta_t)/\mathbb{Q}(\sqrt{-k}))$ is cyclic of order $k-1$ generated by

$$\begin{array}{rcl} \tau : \mathbb{Q}(\zeta_t) & \longrightarrow & \mathbb{Q}(\zeta_t) \\ \zeta_t & \longmapsto & \zeta_t^r \end{array}$$

because the order of r modulo t is $k-1$. Hence $\tau(\Gamma_\nu) = \Gamma_\nu$ since $c_j = c_{rj}$ as in the previous section. So $g(\chi^\nu) \in \mathbb{Q}(\sqrt{-k})$. Let θ denote the Stickelberger element for $\mathbb{Q}(\zeta_t)/\mathbb{Q}$. By Stickelberger's theorem

$$\left(g(\chi^{-1})^t\right) = \tilde{\mathfrak{p}}_1^{t\theta}.$$

$Gal(\mathbb{Q}(\zeta_t)/\mathbb{Q}(\sqrt{-k})) = \{\sigma_b | b \equiv r^i \pmod t,\ i = 1, 2, \cdots, k-1\}$ fixes $\tilde{\mathfrak{p}}_1$. Let $\sum_{i=1}^{k-1} (r^i \pmod t) = \alpha t$ and $(\sum_{(b,t)=1} b) - \alpha t = (k-1)t - \alpha t = \beta t$ for some integers $\alpha, \beta \geq 1$. Then

$$\left(g(\chi^{-1})\right) = \tilde{\mathfrak{p}}_1^\alpha \tilde{\mathfrak{p}}_2^\beta \subset \mathbb{Z}[\zeta_t].$$

Hence

$$\begin{aligned}\Big(g(\chi)\Big) &= \mathfrak{p}_1^{\beta}\mathfrak{p}_2^{\alpha}\\ \Big(g(\chi^{-1})\Big) &= \mathfrak{p}_1^{\alpha}\mathfrak{p}_2^{\beta}\end{aligned}$$

as ideals in $\mathbb{Z}[\sqrt{-k}]$.

Let ψ be a multiplicative character $\psi : (\mathbb{Z}/t\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}$ such that

$$\psi(a) = \begin{cases} 1 & \text{if } a \equiv r^i \pmod t \text{ for some } i,\\ -1 & \text{otherwise.}\end{cases}$$

Then $\mathbb{Q}(\sqrt{-k})$ is the field belonging to ψ.

Lemma 3.1.2. $\psi(-1) = -1$.

Proof. If $-1 \equiv r^i \pmod{4k}$ for some i. Then $i = \frac{k-1}{2}$ because the order of r is $k-1$. But

$$r \equiv 3 \pmod 4 \Rightarrow r^2 \equiv 1 \pmod 4 \Rightarrow r^{2(\frac{k-1}{4})} \equiv 1 \pmod 4.$$

It is a contradiction. □

Apply the analytic class number formula to $\mathbb{Q}(\sqrt{-k})$ and take the absolute value. Then

$$\begin{aligned}\left|\frac{2\pi h}{2\sqrt{t}}\right| &= \Big|L(1,\psi)\Big|\\ &= \pi\frac{\sqrt{t}}{t}\frac{1}{t}\left|\sum_{i=1}^{t-1}\bar{\psi}(a)a\right| = \frac{\pi}{t\sqrt{t}}\Big|\alpha t - \beta t\Big|.\end{aligned}$$

So $h = |\alpha - \beta|$.

Let Π be a $(p-1)$-st root of $-p$. Then Gross-Koblitz formula is

$$g(\omega^d) = (-p)^{k-1}\Pi^{-s(d)}\prod_{j=0}^{k-2}\Gamma_p\Big(1 - \Big\langle\frac{p^j d}{q-1}\Big\rangle\Big).$$

Lemma 3.1.3. *If* $d = \frac{q-1}{t}(t-1) = d_0 + d_1 p + \cdots + d_{k-2}p^{k-2}$ *and* $d' = \frac{q-1}{t} = d_0' + d_1' p + \cdots + d_{k-2}' p^{k-2}$*, then*

$$\begin{aligned} g(\chi^{-1}) &= (-p)^{\alpha}\prod_{j=0}^{k-2}\Gamma_p\Big(1 - \Big\langle\frac{p^j d}{q-1}\Big\rangle\Big)\\ g(\chi) &= (-p)^{\beta}\prod_{j=0}^{k-2}\Gamma_p\Big(1 - \Big\langle\frac{p^j d'}{q-1}\Big\rangle\Big).\end{aligned}$$

Proof. See the proof of Lemma 2.2.3. □

3.2. Main Result

Theorem 3.2.1. *Suppose that $t = 4k$ for a prime $k \equiv 1 \pmod 4$ and that $r \equiv 3 \pmod 4$ is a quadratic non-residue modulo k and its order is $\frac{\phi(t)}{2} = k-1$. Let h be the class number of $\mathbb{Q}(\sqrt{-k})$ and $p = tn + r$ be a prime. Let $p = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathbb{Z}[\sqrt{-k}]$, $\mathfrak{p}_1^h = (a + b\sqrt{-k})$, $\sum_{i=1}^{k-1}(r^i \pmod t) = \alpha t$, $\beta = (k-1) - \alpha$, $d = (\frac{q-1}{t})(t-1) = \sum_{j=0}^{k-2} d_j p^j$ and $d' = (\frac{q-1}{t}) = \sum_{j=0}^{k-2} d'_j p^j$ as in the previous section. Then*

1. $p^h = a^2 + kb^2$;
2. $$2a \equiv \begin{cases} \pm \prod_{j=0}^{k-2} (d_j)! \pmod p & \text{if } \alpha < \beta, \\ \pm \prod_{j=0}^{k-2} (d'_j)! \pmod p & \text{if } \beta < \alpha. \end{cases}$$

Proof. See the proof of Theorem 2.3.1. □

Example 3.2.2. Let $k = 5$, then $\alpha = 1, \beta = 3$ so $h(\mathbb{Q}(\sqrt{-5})) = 2$. Let p be a prime of the form $20n+3$ or $20n+7$ and $d = 19(p^4-1)/20$. Then

$$d = \begin{cases} (13n+1) + (11n+1)p + (17n+2)p^2 + (19n+2)p^3 \\ \qquad\qquad \text{if } p = 20n+3, \\ (17n+5) + (11n+3)p + (13n+4)p^2 + (19n+6)p^3 \\ \qquad\qquad \text{if } p = 20n+7. \end{cases}$$

By Theorem 3.2.1, if $p^2 = a^2 + 5b^2$, then

$$2a \equiv \begin{cases} \pm(13n+1)!(11n+1)!(17n+2)!(19n+2)! \pmod p \\ \qquad\qquad \text{if } p = 20n+3, \\ \pm(17n+5)!(11n+3)!(13n+4)!(19n+6)! \pmod p \\ \qquad\qquad \text{if } p = 20n+7. \end{cases}$$

By Wilson's theorem,

$$2a \equiv \begin{cases} \pm\binom{4n}{n}\binom{11n+1}{4n} \pmod p & \text{if } p = 20n+3, \\ \pm\binom{4n+1}{n}\binom{11n+3}{4n+1} \pmod p & \text{if } p = 20n+7. \end{cases}$$

At the time of the publication of this paper, we could remove the sign ambiguity of our results in [8]. Moreover we generalized our results to the primes of the form of $p = tn + r$ such that p splits in $\mathbb{Q}(\sqrt{-t})$ [9].

References

[1] Allan Adler, *Eisenstein and the Jacobian Varieties of Fermat Curves*, Rocky Mountain Journal of Mathematics, **27** (no. 1) Winter (1997), 1–60.

[2] Gotthold Eisenstein, *Zur Theorie der Quadratische Zerfallung der Primzahlen* $8n+3, 7n+2$ *und* $7n+4$, Crelle, **37** (1948), 97–126 [Math. Werke II, pp. 506–535, art. 33].

[3] Carl Friedrich Gauss, *Theoria Residuorum Biquadraticorum*, Comment. I, Comment. soc. reg. sci. Gottingensis rec., **6** (1828), 27 [Werke, vol. II, pp. 89–90].

[4] Richard H. Hudson and Kenneth S. Williams, *Binomial Coefficients and Jacobi Sums*, Trans. of the Amer. Math. Soc., **281** (no. 2) February (1984), 431–505.

[5] C.G.J. Jacobi, *De Residuis Cubics Commentatio Numerosa*, J. Reine Angew. Math., **2** (1827), 66–69.

[6] C.G.J. Jacobi, *Uber die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, J. Reine Angew. Math., **30** (1846), 166–182.

[7] Serge Lang, Cyclotomic Fields I and II, Springer-Verlag, GTM 121, 1990.

[8] D.H. Lee and S.G. Hahn, *Some congruences for binomial coefficients. II*, Proc. Japan Acad., **76**, Ser. A (2000), 104–107.

[9] D.H. Lee and S.G. Hahn, *Gauss sums and binomial coefficients*, J. Number Theory (2000); submitted.

[10] Lawrence C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, GTM 83, 1997.

Sang Geun Hahn
Department of Mathematics
KAIST
Yusong-Gu Kusong-Dong 373-1
Taejon 305-701
South Korea
E-mail address: `sghahn@math.kaist.ac.kr`

Dong Hoon Lee
Department of Mathematics
KAIST
Yusong-Gu Kusong-Dong 373-1
Taejon 305-701
South Korea
E-mail address: `dhlee@math.kaist.ac.kr`