Proc. Amer. Math. Soc. 134(2006), no. 8, 2213–2222.

BINOMIAL COEFFICIENTS AND QUADRATIC FIELDS

Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn http://pweb.nju.edu.cn/zwsun

Abstract. Let E be a real quadratic field with discriminant $d \not\equiv 0 \pmod p$ where p is an odd prime. For $\rho = \pm 1$ we determine $\prod_{0<c<d,\ (\frac{d}{c})=\rho}\binom{p-1}{\lfloor pc/d\rfloor}$ modulo p^2 in terms of a Lucas sequence, the fundamental unit and the class number of E.

1. Introduction

Let p be an odd prime not dividing a positive integer m. A. Granville [G, (1.15)] discovered the remarkable congruence

$$\prod_{0<k<m}\binom{p-1}{\lfloor pk/m\rfloor} \equiv (-1)^{(m-1)(p-1)/2}(m^p - m + 1) \pmod{p^2},$$

where we use $\lfloor x\rfloor$ to denote the integral part of a real number x. Subsequently the present author [S1] determined further $\prod_{0<k<m/2}\binom{p-1}{\lfloor pk/m\rfloor}$ mod p^2. In this paper a more sophisticated result connected with real quadratic fields will be established.

For $A, B \in \mathbb{Z}$ the Lucas sequences $u_n = u_n(A,B)$ and $v_n = v_n(A,B)$ $(n = 0,1,2,\ldots)$ are given by

$$u_0 = 0,\ u_1 = 1,\ \text{and } u_{n+1} = Au_n - Bu_{n-1} \text{ for } n = 1,2,3,\ldots,$$
$$v_0 = 2,\ v_1 = A,\ \text{and } v_{n+1} = Av_n - Bv_{n-1} \text{ for } n = 1,2,3,\ldots.$$

It is well known that

$$(\alpha-\beta)u_n = \alpha^n - \beta^n \quad\text{and}\quad v_n = \alpha^n + \beta^n \quad \text{for every } n = 0,1,2,\ldots,$$

where α and β are the two roots of the equation $x^2 - Ax + B = 0$. Also, for any odd prime p we have $u_p \equiv (\frac{\Delta}{p}) \pmod p$ and $v_p \equiv A \pmod p$, where $\Delta = A^2 - 4B$ and

2000 *Mathematics Subject Classifications.* Primary 11B65; Secondary 11B37, 11B68, 11R11.

The author was supported by the National Science Fund for Distinguished Young Scholars (No. 10425103) and the Key Program of NSF (No. 10331020) in China.

$(\frac{\cdot}{p})$ denotes the Legendre symbol. (See, e.g., [R, pp. 41-55].) If p is an odd prime not dividing B, then $p \mid u_{p-(\frac{\Delta}{p})}$ since $Au_p + v_p = 2u_{p+1}$ and $Au_p - v_p = 2Bu_{p-1}$.

Throughout this paper, for an assertion P we set

$$[P] = \begin{cases} 1 & \text{if } P \text{ holds,} \\ 0 & \text{otherwise.} \end{cases} \tag{1.1}$$

Our main result is as follows.

Theorem 1.1. *Let E be a quadratic field with discriminant $d = 2^\alpha p_1 \cdots p_r$ where $\alpha \in \{0, 2, 3\}$ and $p_1, \ldots, p_r$ are distinct odd primes. Let $\varepsilon = (a + b\sqrt{d})/2$ be the fundamental unit of the field E where $a, b \in \mathbb{Z}$, and $N(\varepsilon)$ be the norm $(a^2 - b^2 d)/4$ of ε with respect to the field extension $E/\mathbb{Q}$. Let h be the class number of the field E, and p be an odd prime not dividing d. Then, for $\rho = \pm 1$ we have*

$$\begin{aligned}\prod_{\substack{0<c<d\\ (\frac{d}{c})=\rho}} \binom{p-1}{\lfloor pc/d \rfloor} \equiv &1 + \frac{\varphi(d)}{2}\bigg((\alpha + [\alpha > 0])(2^{p-1} - 1) + \sum_{0<i\leqslant r} \frac{p_i^p - p_i}{p_i - 1}\bigg) \\ &+ \frac{\rho}{2}\left(\frac{d}{p}\right)^{[N(\varepsilon)=1]} u_{p-(\frac{d}{p})}(a, N(\varepsilon)) bdh \pmod{p^2},\end{aligned} \tag{1.2}$$

where φ is Euler's totient function and $(\frac{d}{\cdot})$ is the Kronecker symbol.

Remark. Under the conditions of Theorem 1.1, $d \equiv 1 \pmod 4$ if $\alpha = 0$, and $d/4 \equiv 3 \pmod 4$ if $\alpha = 2$; also p divides $bu_{p-(\frac{d}{p})}(a, N(\varepsilon))$ since for $p \nmid b$ we have

$$\left(\frac{a^2 - 4N(\varepsilon)}{p}\right) = \left(\frac{b^2 d}{p}\right) = \left(\frac{d}{p}\right).$$

Example. Each of the quadratic fields $\mathbb{Q}(\sqrt{13}), \mathbb{Q}(\sqrt{21}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{7})$ has class number 1, and their fundamental units are

$$\frac{3+\sqrt{13}}{2},\ \frac{5+\sqrt{21}}{2},\ 5+2\sqrt{6} = \frac{10+2\sqrt{24}}{2},\ 8+3\sqrt{7} = \frac{16+3\sqrt{28}}{2}$$

with norms $-1, 1, 1, 1$ respectively; see, e.g., [C, p. 271]. Let p be an odd prime and $\rho \in \{1, -1\}$. If p does not divide 13, 21, 6, and 7, respectively, then Theorem 1.1

gives the congruences

$$\prod_{\substack{0<c<13\\ (\frac{13}{c})=\rho}} \binom{p-1}{\lfloor pc/13\rfloor} \equiv 1+\frac{13^p-13}{2}+\rho\frac{13}{2}u_{p-(\frac{13}{p})}(3,-1),$$

$$\prod_{\substack{0<c<21\\ (\frac{21}{c})=\rho}} \binom{p-1}{\lfloor pc/21\rfloor} \equiv 1+3(3^p-3)+7^p-7+\rho\left(\frac{21}{p}\right)\frac{21}{2}u_{p-(\frac{21}{p})}(5,1),$$

$$\prod_{\substack{0<c<24\\ 2\nmid c,\ (\frac{6}{c})=\rho}} \binom{p-1}{\lfloor pc/24\rfloor} \equiv 1+8(2^p-2)+2(3^p-3)+\rho\left(\frac{6}{p}\right)24u_{p-(\frac{6}{p})}(10,1),$$

$$\prod_{\substack{0<c<28\\ 2\nmid c,\ (\frac{7}{c})=\rho}} \binom{p-1}{\lfloor pc/28\rfloor} \equiv 1+9(2^p-2)+7^p-7+\rho\left(\frac{7}{p}\right)42u_{p-(\frac{7}{p})}(16,1)$$

modulo p^2 respectively, where $(\frac{6}{c})$ and $(\frac{7}{c})$ are Jacobi symbols.

We deduce Theorem 1.1 by combining the following two theorems.

Theorem 1.2. *Let $m>2$ be an integer with the factorization $p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ where $p_1,\ldots,p_r$ are distinct primes and $\alpha_1,\ldots,\alpha_r$ are positive integers. Let p be an odd prime not dividing m. Then*

$$\begin{aligned}(-1)^{\frac{\varphi(m)}{2}\cdot\frac{p-1}{2}}\left(\frac{p_1}{p}\right)^{[r=1]}&\prod_{\substack{0<k<m/2\\ (k,m)=1}}\binom{p-1}{\lfloor pk/m\rfloor}\\ &\equiv 1+\frac{\varphi(m)}{2}\sum_{i=1}^{r}(\alpha_i p_i-\alpha_i+1)\frac{p_i^{p-1}-1}{p_i-1}\pmod{p^2}.\end{aligned}\tag{1.3}$$

In the next theorem we use the Bernoulli polynomial $B_n(x)$ of degree n and the nth Bernoulli number $B_n=B_n(0)$. Also, we let $\mathbb{P}$ denote the set of all (positive) primes.

Theorem 1.3. *Let E be a real quadratic field with discriminant d and class number h. Let $\varepsilon=(a+b\sqrt{d})/2>1$ be the fundamental unit of E where $a,b\in\mathbb{Z}$, and $N(\varepsilon)$ be the norm $(a^2-b^2d)/4$ of ε. Let p be an odd prime not dividing d, and let u stand for $bu_{p-(\frac{d}{p})}(a,N(\varepsilon))$. Then*

$$\sum_{c=1}^{d-1}\left(\frac{d}{c}\right)\left(B_{p-1}\left(\frac{c}{d}\right)-B_{p-1}\right)\equiv\left(\frac{d}{p}\right)^{[N(\varepsilon)=-1]}dh\frac{u}{p}\pmod{p},\tag{1.4}$$

and

$$\prod_{\substack{0<c<d/2\\(c,d)=1}} \binom{p-1}{\lfloor pc/d\rfloor}^{(\frac{d}{c})} \equiv \begin{cases} (\frac{d}{p})(1+\frac{dhu}{2}) \pmod{p^2} & \text{if } d=8 \text{ or } d\in\mathbb{P},\\ 1+(\frac{d}{p})^{[N(\varepsilon)=1]}\frac{dhu}{2} \pmod{p^2} & \text{otherwise.}\end{cases} \tag{1.5}$$

Remark. In the case where $d\equiv 1 \pmod 4$ is a prime, (1.4) was proved in [GS] by means of p-adic logarithms and Dirichlet's class number formula (see, e.g., [W]).

In the spirit of R. Crandall and C. Pomerance [CP], Theorems 1.1–1.3 might be of computational interest.

We shall make some preparations in the next section and give proofs of Theorems 1.1–1.3 in Section 3.

2. On the sum $\sum_{\substack{0<k<p\\ m\mid k-r}}\frac{1}{k}$ modulo p

Bernoulli polynomials play important roles in many aspects. The reader is referred to [IR, pp. 228-248] for basic properties, and to [DSS] for a bibliography of related papers.

In this section we prove the following basic result and derive some consequences.

Theorem 2.1. *Let m be a positive integer not divisible by an odd prime p. Then for any $r\in\mathbb{Z}$ we have*

$$\sum_{\substack{k=1\\ k\equiv r \pmod m}}^{p-1}\frac{1}{k}\equiv\frac{1}{m}\left(B_{p-1}\left(\left\{\frac{r}{m}\right\}\right)-B_{p-1}\left(\left\{\frac{r-p}{m}\right\}\right)\right) \pmod p, \tag{2.1}$$

where $\{x\}$ stands for the fractional part of a real number x.

Proof. Applying Lemma 3.1 of [S3] with $k=p-2$, we find that

$$-m\sum_{\substack{j=1\\ j\equiv r \pmod m}}^{p-1}\frac{1}{j}\equiv B_{p-1}\left(\frac{p}{m}+\left\{\frac{r-p}{m}\right\}\right)-B_{p-1}\left(\left\{\frac{r}{m}\right\}\right) \pmod p.$$

For $t=\{(r-p)/m\}$, we have

$$B_{p-1}\left(\frac{p}{m}+t\right)-B_{p-1}(t)=\sum_{l=1}^{p-1}\binom{p-1}{l}B_{p-1-l}\left(\left(\frac{p}{m}+t\right)^l-t^l\right)\equiv 0 \pmod p.$$

(Recall that $B_1=-1/2$ and $B_{2n+1}=0$ for $n=1,2,\ldots$. Also, p divides no denominators of $B_0,B_2,\ldots,B_{p-3}$ by the theorem of Clausen and von Staudt (cf. [IR, pp. 233-236]).) Therefore (2.1) follows. □

Remark. The author first discovered Theorem 2.1 in Sept. 1991 by using Fourier series, and Lemma 3.1 of [S3] was originally motivated by this result.

Corollary 2.1. *Let m and n be positive integers, and let p be an odd prime not dividing m. Then*

$$B_{p-1}\left(\left\{\frac{pn}{m}\right\}\right) - B_{p-1} \equiv m\sum_{r=1}^{n} K_p(r,m) \equiv -\sum_{\substack{k=1\\ p\nmid k}}^{\lfloor pn/m\rfloor} \frac{1}{k} \pmod p, \tag{2.2}$$

where

$$K_p(r,m) := \sum_{\substack{k=1\\ m\mid k-rp}}^{p-1} \frac{1}{k} = \sum_{\substack{l=1\\ m\mid l-(1-r)p}}^{p-1} \frac{1}{p-l} \equiv -K_p(1-r,m) \pmod p. \tag{2.3}$$

Proof. In view of Theorem 2.1,

$$\begin{aligned} m\sum_{r=1}^{n} K_p(r,m) \equiv& \sum_{r=1}^{n}\left(B_{p-1}\left(\left\{\frac{rp}{m}\right\}\right) - B_{p-1}\left(\left\{\frac{(r-1)p}{m}\right\}\right)\right) \\ \equiv& B_{p-1}\left(\left\{\frac{pn}{m}\right\}\right) - B_{p-1} \pmod p. \end{aligned}$$

On the other hand,

$$-\sum_{r=1}^{n} K_p(r,m) \equiv \sum_{r=1}^{n}\sum_{\substack{k=1\\ m\mid rp-k}}^{p-1} \frac{1}{rp-k} = \sum_{\substack{j=1\\ p\nmid j,\ m\mid j}}^{pn-1} \frac{1}{j} = \sum_{\substack{k=1\\ p\nmid k}}^{\lfloor pn/m\rfloor} \frac{1}{km} \pmod p.$$

So we have (2.2). □

Let p be an odd prime and r be any integer. An explicit congruence for $K_p(r,12)$ mod p appeared in Corollary 3.3 of [S2]. By Theorem 2.1 and [GS, (4)] we can also determine

$$K_p(3+6r,24),\ K_p(5,40),\ K_p(25,40),\ K_p(6,60),\ K_p(36,60)$$

modulo p in terms of some second-order linear recurrences.

For a prime p and any $a\in\mathbb{Z}$ not divisible by p, the Fermat quotient $q_p(a)$ is defined as the integer $(a^{p-1}-1)/p$.

Corollary 2.2. *Let p be an odd prime and let m be a positive integer not divisible by p. Then we have*

$$\sum_{r=1}^{m} rK_p(r,m) \equiv -q_p(m) \pmod p. \tag{2.4}$$

Proof. By Corollary 2.1,

$$\begin{aligned}\sum_{n=1}^{m}\sum_{r=1}^{n}K_p(r,m)\equiv&\frac{1}{m}\sum_{n=1}^{m}\left(B_{p-1}\left(\left\{\frac{pn}{m}\right\}\right)-B_{p-1}\right)\\ \equiv&m^{p-2}\left(\sum_{n=1}^{m}B_{p-1}\left(\left\{\frac{pn}{m}\right\}\right)-mB_{p-1}\right)\\ \equiv&\sum_{r=0}^{m-1}m^{p-2}B_{p-1}\left(\frac{r}{m}\right)-m^{p-1}B_{p-1}=(1-m^{p-1})B_{p-1}\pmod p\end{aligned}$$

where we have applied Raabe's theorem in the last step. It is well known that $pB_{p-1}\equiv -1\pmod p$ (cf. [IR, p. 233]). Also,

$$\begin{aligned}&\sum_{n=1}^{m}\sum_{r=1}^{n}K_p(r,m)=\sum_{r=1}^{m}(m-(r-1))K_p(r,m)\\ \equiv&-\sum_{r=1}^{m}(m+1-r)K_p(m+1-r,m)=-\sum_{s=1}^{m}sK_p(s,m)\pmod p.\end{aligned}$$

So we have (2.4). □

Remark. It can be shown that (2.4) is equivalent to a formula of Lerch [L] which was deduced in a different way.

3. Proofs of Theorems 1.1–1.3

Proof of Theorem 1.2. For each positive integer d we set

$$\psi(d)=\prod_{\substack{0<c<d/2\\(c,d)=1}}\binom{p-1}{\lfloor pc/d\rfloor},$$

where $\psi(1)$ and $\psi(2)$ are considered as 1. For any $a\in\mathbb{Z}$ with $p\nmid a$, clearly

$$\begin{aligned}a^p-a=&a\left(a^{(p-1)/2}+\left(\frac{a}{p}\right)\right)\left(a^{(p-1)/2}-\left(\frac{a}{p}\right)\right)\\ \equiv&2a\left(\frac{a}{p}\right)\left(a^{(p-1)/2}-\left(\frac{a}{p}\right)\right)\pmod{p^2}.\end{aligned}$$

Thus, Theorem 1.1 of [S1] implies that if $d\not\equiv 0\pmod p$ then

$$\begin{aligned}&(-1)^{\frac{p-1}{2}\lfloor\frac{d-1}{2}\rfloor}\prod_{0<c<d/2}\binom{p-1}{\lfloor pc/d\rfloor}\\ \equiv&\begin{cases}(\frac{d}{p})+(\frac{d}{p})\frac{d^p-d}{2}&\text{if }2\nmid d,\\ (\frac{2d}{p})+(\frac{2d}{p})\frac{d^p-d}{2}-(\frac{2d}{p})\frac{2^p-2}{2}&\text{if }2\mid d,\end{cases}\\ \equiv&\left(\frac{d}{p}\right)\left(\frac{2}{p}\right)^{[2\mid d]}\left(1+\frac{d^p-d}{2}-[2\mid d](2^{p-1}-1)\right)\pmod{p^2}.\end{aligned}$$

Since $\prod_{0<k<n/2}\binom{p-1}{\lfloor pk/n\rfloor}=\prod_{d\mid n}\psi(d)$ for $n=1,2,\dots$, applying the Möbius inversion formula we get that

$$\begin{aligned}\psi(m)=&\prod_{d\mid m}\prod_{0<c<d/2}\binom{p-1}{\lfloor pc/d\rfloor}^{\mu(m/d)}\\ \equiv&(-1)^{\frac{p-1}{2}\sum_{d\mid m}\mu(\frac{m}{d})(\frac{d-1}{2}-\frac{[2\mid d]}{2})}\left(\frac{2}{p}\right)^{\sum_{d\mid m}\mu(m/d)[2\mid d]}\\ &\times\prod_{d\mid m}\left(\frac{d}{p}\right)^{\mu(m/d)}\times\prod_{d\mid m}\left(1+\mu\left(\frac{m}{d}\right)\left(\frac{d^p-d}{2}-[2\mid d](2^{p-1}-1)\right)\right)\pmod{p^2}.\end{aligned}$$

By elementary number theory, $\sum_{d\mid m}\mu(\frac{m}{d})\frac{d-1}{2}=\frac{\varphi(m)}{2}$ and also

$$\sum_{d\mid m}\mu\left(\frac{m}{d}\right)[2\mid d]=\sum_{2c\mid m}\mu\left(\frac{m}{2c}\right)=[2\mid m]\sum_{c\mid(m/2)}\mu\left(\frac{m/2}{c}\right)=0$$

since $m>2$. Therefore

$$(-1)^{\frac{\varphi(m)}{2}\cdot\frac{p-1}{2}}\psi(m)\equiv\prod_{d\mid m}\left(\frac{d}{p}\right)^{\mu(m/d)}\times\left(1+\sum_{d\mid m}\mu\left(\frac{m}{d}\right)\frac{d^p-d}{2}\right)\pmod{p^2}.$$

Observe that

$$\begin{aligned}\prod_{d\mid m}\left(\frac{d}{p}\right)^{\mu(m/d)}&=\prod_{I\subseteq\{1,\dots,r\}}\left(\frac{m/\prod_{i\in I}p_i}{p}\right)^{\mu(\prod_{i\in I}p_i)}\\ &=\left(\frac{m^{2^r}/\prod_{I\subseteq\{1,\dots,r\}}\prod_{i\in I}p_i}{p}\right)=\left(\frac{m^{2^r}/\prod_{i=1}^r p_i^{2^{r-1}}}{p}\right)\\ &=\left(\frac{\prod_{i=1}^r p_i^{2^{r-1}(2\alpha_i-1)}}{p}\right)=\left(\frac{p_1\cdots p_r}{p}\right)^{2^{r-1}}=\left(\frac{p_1}{p}\right)^{[r=1]}.\end{aligned}$$

Also,

$$\begin{aligned}\varphi(m)+\sum_{d\mid m}\mu\left(\frac{m}{d}\right)(d^p-d)=&\sum_{d\mid m}\mu(d)\frac{m^p}{d^p}=m^p\prod_{i=1}^r\left(1-p_i^{-p}\right)\\ =&\prod_{i=1}^r\left(p_i^{\alpha_ip}-p_i^{(\alpha_i-1)p}\right)=\prod_{i=1}^r\left((p_i+(p_i^p-p_i))^{\alpha_i}-(p_i+(p_i^p-p_i))^{\alpha_i-1}\right)\\ \equiv&\prod_{i=1}^r\left(p_i^{\alpha_i}+\alpha_ip_i^{\alpha_i-1}(p_i^p-p_i)-\left(p_i^{\alpha_i-1}+(\alpha_i-1)p_i^{\alpha_i-2}(p_i^p-p_i)\right)\right)\\ \equiv&\prod_{i=1}^r\left(\varphi(p_i^{\alpha_i})+(p_i^{p-1}-1)(\alpha_ip_i^{\alpha_i}-(\alpha_i-1)p_i^{\alpha_i-1})\right)\\ \equiv&\varphi(m)\left(1+\sum_{i=1}^r\frac{p_i^{p-1}-1}{p_i-1}(\alpha_ip_i-\alpha_i+1)\right)\pmod{p^2}.\end{aligned}$$

Thus (1.3) holds in view of the above. $\square$

Proof of Theorem 1.3. Write $\varepsilon^{p-(\frac{d}{p})}=(V+U\sqrt{d})/2$ where $U,V\in\mathbb{Z}$, and let p' be an integer with $pp'\equiv 1\pmod{d}$. Theorem 3.1 of Williams [W] states that

$$h\frac{U}{p}\equiv-\left(\frac{d}{p}\right)N(\varepsilon)^{((\frac{d}{p})-1)/2}\sum_{i=1}^{p-1}\frac{\beta_p(i)}{i}\pmod{p}$$

where $\beta_p(i)=\sum_{0<j<d\{p'i/d\}}(\frac{d}{j})$.

Let $\bar{\varepsilon}=(a-b\sqrt{d})/2$. Then $\varepsilon+\bar{\varepsilon}=a$ and $\varepsilon\bar{\varepsilon}=N(\varepsilon)$. Clearly

$$v_n(a,N(\varepsilon))+u_n(a,N(\varepsilon))b\sqrt{d}=\varepsilon^n+\bar{\varepsilon}^n+\frac{\varepsilon^n-\bar{\varepsilon}^n}{\varepsilon-\bar{\varepsilon}}b\sqrt{d}=2\varepsilon^n$$

for $n=0,1,\ldots$, thus $U=bu_{p-(\frac{d}{p})}(a,N(\varepsilon))=u$ (and $V=v_{p-(\frac{d}{p})}(a,N(\varepsilon))$).

Observe that

$$\begin{aligned}\sum_{i=1}^{p-1}\frac{\beta_p(i)}{i}=&\sum_{j=1}^{d-1}\left(\frac{d}{j}\right)\sum_{\substack{0<i<p\\ d\{p'i/d\}>j}}\frac{1}{i}=\sum_{j=1}^{d-1}\left(\frac{d}{j}\right)\sum_{j<r<d}\sum_{\substack{0<i<p\\ d\mid p'i-r}}\frac{1}{i}\\ =&\sum_{j=1}^{d-1}\left(\frac{d}{j}\right)\sum_{j<r<d}\sum_{\substack{0<i<p\\ d\mid i-rp}}\frac{1}{i}=\sum_{j=1}^{d-1}\left(\frac{d}{j}\right)\sum_{j<r<d}K_p(r,d).\end{aligned}$$

As $\chi(j)=(\frac{d}{j})$ is a nontrivial multiplicative character modulo d, the sum $\sum_{j=1}^{d-1}(\frac{d}{j})$ vanishes. Therefore, with the help of Corollary 2.1, we have

$$\begin{aligned}\sum_{i=1}^{p-1}\frac{\beta_p(i)}{i}=&\sum_{j=1}^{d-1}\left(\frac{d}{j}\right)\left(\sum_{r=1}^{d}K_p(r,d)-\sum_{r=1}^{j}K_p(r,d)\right)\\ \equiv&\sum_{j=1}^{d-1}\left(\frac{d}{j}\right)\frac{1}{d}\left(0-B_{p-1}\left(\left\{\frac{pj}{d}\right\}\right)+B_{p-1}\right)\\ \equiv&-\frac{1}{d}\left(\frac{d}{p}\right)\sum_{j=1}^{d-1}\left(\frac{d}{pj}\right)\left(B_{p-1}\left(\left\{\frac{pj}{d}\right\}\right)-B_{p-1}\right)\\ \equiv&-\frac{1}{d}\left(\frac{d}{p}\right)\sum_{c=1}^{d-1}\left(\frac{d}{c}\right)\left(B_{p-1}\left(\frac{c}{d}\right)-B_{p-1}\right)\pmod{p}.\end{aligned}$$

Combining the above we obtain (1.4).

For each $c = 1, \dots, d-1$, we have $\chi(d-c) = \chi(-1)\chi(c) = \chi(c)$; also

$$\begin{aligned}(-1)^{\lfloor pc/d \rfloor}\binom{p-1}{\lfloor pc/d \rfloor} &= \prod_{k=1}^{\lfloor pc/d \rfloor}\left(1-\frac{p}{k}\right)\\ &\equiv 1 - p\sum_{k=1}^{\lfloor pc/d \rfloor}\frac{1}{k} \equiv 1 + p\Big(B_{p-1}\left(\left\{\frac{pc}{d}\right\}\right) - B_{p-1}\Big) \pmod{p^2}.\end{aligned}$$

Taking the above congruence and (1.3) modulo p, we obtain

$$\begin{aligned}\prod_{\substack{0<c<d/2\\(c,d)=1}}(-1)^{\lfloor pc/d \rfloor} \equiv &\prod_{\substack{0<c<d/2\\(c,d)=1}}\binom{p-1}{\lfloor pc/d \rfloor}\\ \equiv &(-1)^{\frac{\varphi(d)}{2}\cdot\frac{p-1}{2}}\left(\frac{d}{p}\right)^{[d \text{ is a prime power}]} \pmod{p}\end{aligned}$$

and hence

$$\prod_{0<c<d/2}(-1)^{\lfloor pc/d \rfloor (\frac{d}{c})} = \left(\frac{d}{p}\right)^{[d=8 \text{ or } d\in\mathbb{P}]}.$$

(Note that $4 \mid \varphi(d)$ and no square of an odd prime divides d.) On the other hand,

$$\begin{aligned}&\prod_{0<c<d/2}\left((-1)^{\lfloor pc/d \rfloor}\binom{p-1}{\lfloor pc/d \rfloor}\right)^{(\frac{d}{c})}\\ \equiv &\prod_{0<c<d/2}\left(1 + p\left(\frac{d}{c}\right)\left(B_{p-1}\left(\left\{\frac{pc}{d}\right\}\right) - B_{p-1}\right)\right)\\ \equiv &1 + \frac{p}{2}\sum_{0<c<d/2}\left(\frac{d}{c}\right)\left(B_{p-1}\left(\left\{\frac{pc}{d}\right\}\right) - B_{p-1}\right)\\ &+ \frac{p}{2}\sum_{0<c<d/2}\left(\frac{d}{d-c}\right)\left(B_{p-1}\left(\left\{\frac{p(d-c)}{d}\right\}\right) - B_{p-1}\right)\\ \equiv &1 + \frac{p}{2}\sum_{c=1}^{d-1}\left(\frac{d}{c}\right)\left(B_{p-1}\left(\left\{\frac{pc}{d}\right\}\right) - B_{p-1}\right)\\ \equiv &1 + \frac{p}{2}\left(\frac{d}{p}\right)\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)\left(B_{p-1}\left(\frac{r}{d}\right) - B_{p-1}\right) \pmod{p^2}.\end{aligned}$$

These, together with (1.4), yield

$$\prod_{0<c<d/2}\binom{p-1}{\lfloor pc/d \rfloor}^{(\frac{d}{c})} \equiv \left(\frac{d}{p}\right)^{[d=8 \text{ or } d\in\mathbb{P}]}\left(1 + \frac{dhu}{2}\left(\frac{d}{p}\right)^{[N(\varepsilon)=1]}\right) \pmod{p^2}.$$

It is well known that $N(\varepsilon)=-1$ if $d=8$ or $d\in\mathbb{P}$ (see, e.g., [C, pp. 185-186]). So the desired (1.5) follows. $\square$

Proof of Theorem 1.1. By Theorem 1.2 and the proof of Theorem 1.3,

$$\left(\frac{d}{p}\right)^{[d=8\text{ or }d\in\mathbb{P}]}\prod_{\substack{0<c<d/2\\(c,d)=1}}\binom{p-1}{\lfloor pc/d\rfloor}\equiv 1+\frac{\varphi(d)}{2}F(d,p)\pmod{p^2}$$

where

$$\begin{aligned}F(d,p)=&[\alpha>0](2\alpha-\alpha+1)\frac{2^{p-1}-1}{2-1}+\sum_{0<i\leqslant r}(p_i-1+1)\frac{p_i^{p-1}-1}{p_i-1}\\=&(\alpha+[\alpha>0])(2^{p-1}-1)+\sum_{0<i\leqslant r}\frac{p_i^p-p_i}{p_i-1};\end{aligned}$$

also

$$\left(\frac{d}{p}\right)^{[d=8\text{ or }d\in\mathbb{P}]}\prod_{\substack{0<c<d/2\\(c,d)=1}}\binom{p-1}{\lfloor pc/d\rfloor}^{(\frac{d}{c})}\equiv 1+\frac{dhu}{2}\left(\frac{d}{p}\right)^{[N(\varepsilon)=1]}\pmod{p^2}$$

where $u=bu_{p-(\frac{d}{p})}(a,N(\varepsilon))\equiv 0\pmod p$. Therefore

$$\begin{aligned}&\prod_{\substack{0<c<d/2\\(\frac{d}{c})=\rho}}\binom{p-1}{\lfloor pc/d\rfloor}\binom{p-1}{\lfloor p(d-c)/d\rfloor}=\prod_{\substack{0<c<d/2\\(c,d)=1}}\binom{p-1}{\lfloor pc/d\rfloor}^{1+\rho(\frac{d}{c})}\\ \equiv&\left(1+\frac{\varphi(d)}{2}F(d,p)\right)\left(1+\frac{dhu}{2}\left(\frac{d}{p}\right)^{[N(\varepsilon)=1]}\right)^{\rho}\\ \equiv&\left(1+\frac{\varphi(d)}{2}F(d,p)\right)\left(1+\rho\frac{dhu}{2}\left(\frac{d}{p}\right)^{[N(\varepsilon)=1]}\right)\\ \equiv&1+\frac{\varphi(d)}{2}F(d,p)+\rho\frac{dhu}{2}\left(\frac{d}{p}\right)^{[N(\varepsilon)=1]}\pmod{p^2}.\end{aligned}$$

This proves (1.2). We are done. $\square$

Acknowledgment. The author thanks the referee for his many helpful comments.

References

[C] H. Cohn, *Advanced Number Theory*, Dover Publ. Inc., New York, 1962.
[CP] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, New York, 2001.

[DSS] K. Dilcher, L. Skula and I. Sh. Slavutskii, *Bernoulli numbers, 1713/1990*, Queen's Papers in Pure and Appl. Math. **87**(1990). The website of the on-line version is `http://www.mathstat.dal.ca/dilcher/bernoulli.html`.

[G] A. Granville, *Arithmetic properties of binomial coefficients.I. Binomial coefficients modulo prime powers,* in: Organic mathematics (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.

[GS] A. Granville and Z. W. Sun, *Values of Bernoulli polynomials*, Pacific J. Math. **172** (1996), 117–137.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in math.; 84), 2nd ed., Springer, New York, 1990.

[L] M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1}-1)/p = q(a)$, Math. Ann. **60** (1905), 471–490.

[R] P. Ribenboim, *The Book of Prime Number Records*, Springer, New York, 1988.

[S1] Z. W. Sun, *Products of binomial coefficients modulo* p^2, Acta Arith. **97** (2001), 87–98.

[S2] Z. W. Sun, *On the sum* $\sum_{k\equiv r \pmod m}\binom{n}{k}$ *and related congruences*, Israel J. Math. **128** (2002), 135–156.

[S3] Z. W. Sun, *General congruences for Bernoulli polynomials*, Discrete Math. **262** (2003), 253–276.

[W] H. C. Williams, *Some formulae concerning the fundamental unit of a real quadratic field*, Discrete Math. **92** (1991), 431–440.