ACTA ARITHMETICA
103.4 (2002)

A congruence involving the quotients of Euler and its applications (I)

by

Tianxin Cai (Hangzhou)

1. The main result. Let $n, r \geq 2$ be natural numbers with $(n, r) = 1$. Throughout the paper, let χ_n denote the trivial Dirichlet character modulo n and let $q_r(n)$ denote the Euler quotient, i.e.,

$$q_r(n) = \frac{r^{\phi(n)} - 1}{n}.$$

In 1938, E. Lehmer [4] established the following congruence:

$$\sum_{i=1}^{(p-1)/2} \frac{1}{i} \equiv -2q_2(p) + pq_2^2(p) \pmod{p^2} \tag{1}$$

for any odd prime p. This is an improvement of Eisenstein's [2] congruence from 1850,

$$q_2(p) \equiv -\frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{(p-1)/2}\right) \pmod{p}.$$

Using (1) and other similar congruences, E. Lehmer obtained various criteria for the first case of Fermat's Last Theorem (cf. [6]). The proof of (1) followed the method of Glaisher [3], which depends on Bernoulli polynomials of fractional arguments. In this paper, we use an identity proved by Szmidt, Urbanowicz and Zagier [8] to generalize congruence (1) to a congruence modulo an arbitrary positive integer. The main theorem we obtain is the following:

Theorem 1. *For odd $n > 1$, we have*

$$\sum_{i=1}^{(n-1)/2} \frac{\chi_n(i)}{i} \equiv -2q_2(n) + nq_2^2(n) \pmod{n^2}. \tag{2}$$

2000 *Mathematics Subject Classification*: 11A25, 11B65, 11B68.

Key words and phrases: quotients of Euler, Bernoulli polynomials, binomial coefficients.

Partly supported by the project NNSFC.

COROLLARY 1 (Lehmer). *If p is odd prime, then*

$$\sum_{i=1}^{(p-1)/2} \frac{1}{i} \equiv -2q_2(p) + pq_2^2(p) \pmod{p^2}.$$

2. Applications. In 1895, Morley [5] proved for any prime $p \geq 5$ the congruence

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

This is one of the most beautiful and profound congruences concerning binomial coefficients. However, his ingenious proof, which is based on an explicit form of De Moivre's Theorem, cannot be modified to investigate other binomial coefficients. As an application of Theorem 1, we present a generalization of congruence (3), i.e.,

THEOREM 2. *If n is odd, then*

$$(-1)^{\phi(n)/2}\prod_{d|n}\binom{d-1}{(d-1)/2}^{\mu(n/d)} \equiv 4^{\phi(n)} \begin{cases} \pmod{n^3} & \text{for } 3\nmid n, \\ \pmod{n^3/3} & \text{for } 3 \mid n, \end{cases} \tag{4}$$

where $\mu(n)$ is the Möbius function, and $\phi(n)$ is Euler's function.

COROLLARY 2 (Morley). *If $p \geq 5$ is prime, then congruence* (3) *holds.*

COROLLARY 3. *If $p \geq 5$ is prime, then*

$$(-1)^{(p-1)/2}\binom{p^l-1}{(p^l-1)/2}\Big/\binom{p^{l-1}-1}{(p^{l-1}-1)/2} \equiv 4^{\phi(p^l)} \pmod{p^{3l}},$$

and for any $l \geq 1$,

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

REMARK. From Corollary 3 and the fact Crandall, Dilcher and Pomerance have verified that 1093 and 3511 are the only primes less than $4 \cdot 10^{12}$ such that $q_2(p) \equiv 0 \pmod{p}$, it is easy to see that for each $l \geq 1$, there are exactly two primes up to $4 \cdot 10^{12}$ such that

$$\binom{p^l-1}{(p^l-1)/2} \equiv \pm 1 \pmod{p^2},$$

where the plus sign is to be chosen for $p = 1093$ and the minus sign for $p = 3511$ (cf. [7]).

COROLLARY 4. *If $p, q \geq 5$ are distinct odd primes, then*

$$\binom{pq-1}{(pq-1)/2} \equiv 4^{(p-1)(q-1)}\binom{p-1}{(p-1)/2}\binom{q-1}{(q-1)/2} \pmod{p^3q^3}; \tag{5}$$

in particular, *we have*

$$\binom{pq-1}{(pq-1)/2} \equiv \binom{p-1}{(p-1)/2}\binom{q-1}{(q-1)/2} \pmod{pq}. \tag{6}$$

Moreover, as an application of Theorem 1, we have

THEOREM 3. *Let $n \geq 1$ be an integer. Then for any integers $u > v > 0$,*

$$\prod_{d|n}\binom{ud}{vd}^{\mu(n/d)} \equiv 1 \begin{cases} \pmod{n^3} & \text{if } 3 \nmid n,\ n \neq 2^a, \\ \pmod{n^3/3} & \text{if } 3 \mid n, \\ \pmod{n^3/2} & \text{if } n = 2^a,\ a \geq 2, \\ \pmod{n^3/4} & \text{if } n = 2. \end{cases}$$

COROLLARY 5 (Jacobstahl). *If $p \geq 5$ is prime, then*

$$\binom{up}{vp} \Big/ \binom{u}{v} \equiv 1 \pmod{p^3}.$$

COROLLARY 6. *If $p, q \geq 5$ are distinct primes, then for any integers $u > v > 0$,*

$$\binom{up}{vp}\binom{uq}{vq} \equiv \binom{u}{v}\binom{upq}{vpq} \pmod{p^3q^3}.$$

3. The proof of Theorem 1. Before we prove Theorem 1 we recall the identity proved by Szmidt, Urbanowicz and Zagier. Let χ be a Dirichlet character modulo M, N a positive integral multiple of M and r (> 1) a positive integer prime to N. Then for any integer $m \geq 0$ we have

$$(m+1)r^m \sum_{0<n<N/r} \chi(n)n^m = -B_{m+1,\chi}r^m + \frac{\overline{\chi}(r)}{\phi(r)} \sum_{\psi} \overline{\psi}(-N)B_{m+1,\chi\psi}(N), \tag{7}$$

where the sum on the right side is taken over all Dirichlet characters ψ modulo r, and $B_{s,\chi}(X)$ (resp. $B_{s,\chi}$) denotes the sth generalized Bernoulli polynomial (resp. number) attached to χ. Moreover, we have the generalized summation formula for $M \mid N$:

$$\sum_{n=0}^{N-1} \chi(n)n^m = \frac{1}{m+1}(B_{m+1,\chi}(N) - B_{m+1,\chi}). \tag{8}$$

In what follows we set

$$B_{s,\chi}^{[N]} = B_{s,\chi} \prod_{p|(N/M)} (1 - \chi(p)p^{s-1}), \qquad B_{s,\chi}^{[N]}(X) = \sum_{i=1}^{s} \binom{s}{i} B_{s,\chi}^{[N]} X^{s-i}.$$

For natural r prime to n write

$$S_r(n) = \sum_{0<i<n/r} \chi_n(i) i^{n\phi(n)-1}.$$

Proof of Theorem 1. By Euler's theorem we have

$$\sum_{i=1}^{(n-1)/2} \frac{\chi_n(i)}{i} \equiv S_2(n) \pmod{n^2}. \tag{9}$$

In view of (7) with $N = M = n$, $m = n\phi(n) - 1$, $\chi = \chi_n$ and $r = 2$ we obtain

$$n\phi(n)2^{n\phi(n)-1}S_2(n) = (1-2^{n\phi(n)})B_{n\phi(n),\chi_n}(n) + (B^{[2n]}_{n\phi(n),\chi_n}(n) - B^{[2n]}_{n\phi(n),\chi_n}).$$

Hence, by virtue of the evident congruence

$$B^{[2n]}_{n\phi(n),\chi_n}(n) - B^{[2n]}_{n\phi(n),\chi_n} \equiv 0 \pmod{n^3\phi(n)}$$

(which follows from $B^{[2n]}_{s,\chi_n} = B_s \prod_{p|2n}(1-p^{s-1})$ and the von Staudt and Clausen theorem), we deduce that

$$\begin{aligned} S_2(n) &\equiv \frac{2(1-2^{n\phi(n)})}{n\phi(n)} B_{n\phi(n),\chi_n} \\ &\equiv \frac{2(1-2^{n\phi(n)})}{n\phi(n)} B_{n\phi(n)} \prod_{p|n}(1-p^{n\phi(n)-1}) \pmod{n^2}. \end{aligned}$$

Now Theorem 1 follows from (9) and the obvious congruence

$$\frac{n}{\phi(n)} B_{n\phi(n)} \prod_{p|n}(1-p^{n\phi(n)-1}) \equiv 1 \pmod{n^2}$$

(which follows from the evident congruence $pB_{n\phi(n)} \equiv p-1 \pmod{p^{\mathrm{ord}_p(n)}}$, where $p \mid n$) and $2^{\phi(n)} = nq_2(n) + 1$.

4. The proof of Theorem 2. In order to prove Theorems 2 and 3, we need the following

Lemma 1. *Let $n > 1$ be an integer. Then*

$$\sum_{r=1}^{n-1} \frac{\chi_n(r)}{r^2} \equiv 0 \begin{cases} \pmod{n} & \text{if } 3 \nmid n,\ n \neq 2^a, \\ \pmod{n/3} & \text{if } 3 \mid n, \\ \pmod{n/2} & \text{if } n = 2^a. \end{cases} \tag{10}$$

Proof. By Euler's theorem we have

$$\sum_{i=1}^{n-1} \frac{\chi_n(i)}{i^2} \equiv \sum_{i=1}^{n-1} \chi_n(i) i^{\phi(n)-2} \pmod{n}.$$

Denote the right side of the above congruence by $T(n)$. By (8) we have

$$T(n) = \frac{1}{\phi(n)-1}(B_{\phi(n)-1,\chi_n}(n) - B_{\phi(n)-1,\chi_n}),$$

and so by the von Staudt and Clausen theorem we obtain

$$T(n) = \frac{1}{\phi(n)-1}\sum_{k=1}^{\phi(n)-2}\binom{\phi(n)-1}{k}B_{\phi(n)-1-k,\chi_n}n^k \equiv B_{\phi(n)-2,\chi_n}n \pmod n$$

because

$$B_{s,\chi_n} = \prod_{p|n}(1-p^{s-1})B_s.$$

Thus, by the above equation and the von Staudt and Clausen theorem, we see that $B_{\phi(n)-2,\chi_n}$ is a p-integral rational number for $p \,|\, n$ unless $p-1 \,|\, \phi(n)-2$. If $p \,|\, n$ we have $p-1 \,|\, \phi(n)$, and so $p-1 \,|\, 2$, i.e., $p = 2$ or 3. Hence Lemma 1 follows easily. ∎

Proof of Theorem 2. Define

$$A_n = \binom{n-1}{(n-1)/2}.$$

Then

$$A_n = \prod_{r=1}^{(n-1)/2}\frac{n-r}{r} = \prod_{d|n}\prod_{\substack{r=1\\(r,n)=d}}^{(n-1)/2}\frac{n-r}{r} = \prod_{d|n}T_{n/d} = \prod_{d|n}T_d,$$

where

$$T_d = \prod_{\substack{r=1\\(r,d)=1}}^{(d-1)/2}\frac{d-r}{r}.$$

By using the inverse formula for the Möbius function, we have

$$T_n = \prod_{d|n}A_d^{\mu(n/d)} = \prod_{d|n}\binom{d-1}{(d-1)/2}^{\mu(n/d)}.$$

On the other hand,

$$\begin{aligned}(11)\qquad T_n &= \prod_{\substack{r=1\\(r,n)=1}}^{(n-1)/2}\frac{n-r}{r} = (-1)^{\phi(n)/2}\prod_{\substack{r=1\\(r,n)=1}}^{(n-1)/2}\left(1-\frac{n}{r}\right)\\ &= (-1)^{\phi(n)/2}\Bigg\{1 - n\sum_{\substack{r=1\\(r,n)=1}}^{(n-1)/2}\frac{1}{r}\\ &\quad + \frac{n^2}{2}\left\{\left(\sum_{\substack{r=1\\(r,n)=1}}^{(n-1)/2}\frac{1}{r}\right)^2 - \sum_{\substack{r=1\\(r,n)=1}}^{(n-1)/2}\frac{1}{r^2}\right\}\Bigg\} \pmod{n^3}.\end{aligned}$$

Noting that

$$(12)\qquad \sum_{\substack{r=1\\(r,n)=1}}^{[n/2]} \frac{1}{r^2} \equiv \frac{1}{2} \sum_{\substack{r=1\\(r,n)=1}}^{[n/2]} \left(\frac{1}{r^2} + \frac{1}{(n-r)^2}\right) \equiv \frac{1}{2} \sum_{\substack{r=1\\(r,n)=1}}^{n-1} \frac{1}{r^2} \pmod n,$$

applying Theorem 1 and Lemma 1 to (11), we have

$$\prod_{d|n} \binom{d-1}{(d-1)/2}^{\mu(n/d)} \equiv (-1)^{\phi(n)/2}(1+nq_2(n))^2 \equiv (-1)^{\phi(n)/2}4^{\phi(n)} \pmod{n^3}$$

for $3 \nmid n$; if $3 \mid n$, the modulus must be replaced by $n^3/3$. This completes the proof of Theorem 2.

Corollary 3 follows by using Theorem 2 repeatedly. As for Corollary 4, we only need to deal with the case $p = 3$, $q > 3$. If $q \equiv 2 \pmod 3$, then

$$\binom{q-1}{(q-1)/2} \equiv 0 \pmod 3,$$

since $[(q-1)/3] - 2[(q-1)/6] = 1$, hence (5) is true. If $q \equiv 1 \pmod 3$, it follows from Fermat's Theorem that

$$\sum_{\substack{r=1\\(r,6q)=1}}^{3q-1} \frac{1}{r^3} \equiv \sum_{\substack{r=1\\(r,2q)=1}}^{3q-1} r \equiv \sum_{\substack{r=1\\2\nmid r}}^{3q-1} r - q = \frac{(3q-1)^2}{4} - q \equiv 0 \pmod 3.$$

This improves (10) (the case $n = 3q$) to

$$\sum_{r=1}^{3q-1} \frac{\chi_{3q}(r)}{r^2} \equiv 0 \pmod{3q}.$$

Therefore (5) follows immediately from the proof of Theorem 2.

Remark. Congruence (6) was also proved in [1].

5. The proof of Theorem 3. We follow the proof of Theorem 2. Define

$$D_n = \binom{un}{vn}.$$

Then

$$D_n = \frac{u}{v}\binom{un-1}{vn-1} = \frac{u}{v}\prod_{d|n} \prod_{\substack{r=1\\(r,n)=d}}^{vn-1} \frac{un-r}{r} = \frac{u}{v}\prod_{d|n} V_{n/d} = \frac{u}{v}\prod_{d|n} V_d,$$

where

$$V_d = \prod_{\substack{r=1\\(r,d)=1}}^{vd-1} \frac{ud-r}{r}.$$

By using the inverse formula for the Möbius function, we have

$$V_n = \prod_{d|n} D_d^{\mu(n/d)} = \prod_{d|n} \binom{ud}{vd}^{\mu(n/d)}.$$

On the other hand,

$$V_n = \prod_{\substack{r=1\\(r,n)=1}}^{vn-1} \frac{un-r}{r} = (-1)^{v\phi(n)} \prod_{\substack{r=1\\(r,d)=1}}^{vd-1} \left(1-\frac{un}{r}\right) \tag{13}$$

$$\equiv (-1)^{v\phi(n)} \Bigg\{ 1 - un \sum_{\substack{r=1\\(r,n)=1}}^{vn-1} \frac{1}{r} + \frac{u^2n^2}{2} \Bigg\{ \Bigg(\sum_{\substack{r=1\\(r,n)=1}}^{vn-1} \frac{1}{r} \Bigg)^2 - \sum_{\substack{r=1\\(r,n)=1}}^{vn-1} \frac{1}{r^2} \Bigg\} \Bigg\} \pmod{n^3}.$$

Since

$$\sum_{\substack{r=1\\(r,n)=1}}^{vn-1} \frac{1}{r^2} \equiv v \sum_{\substack{r=1\\(r,n)=1}}^{n-1} \frac{1}{r^2} \pmod{n},$$

and

$$\sum_{\substack{r=1\\(r,n)=1}}^{vn-1} \frac{1}{r} = \sum_{i=0}^{v-1} \sum_{\substack{r=1\\(r,n)=1}}^{n-1} \frac{1}{r+in} = \sum_{i=0}^{v-1} \sum_{\substack{r=1\\(r,n)=1}}^{[n/2]} \left(\frac{1}{r+in} + \frac{1}{(i+1)n-r} \right)$$

$$\equiv -n \sum_{i=0}^{v-1} (2i+1) \sum_{\substack{r=1\\(r,n)=1}}^{[n/2]} \frac{1}{r^2} \equiv -v^2 n \sum_{\substack{r=1\\(r,n)=1}}^{[n/2]} \frac{1}{r^2} \pmod{n^2},$$

it follows from (12) and (13) that

$$V_n \equiv (-1)^{v\phi(n)} \Bigg\{ 1 + \frac{uv(u-v)}{2} \sum_{\substack{r=1\\(r,n)=1}}^{n-1} \frac{1}{r^2} \Bigg\} \pmod{n^3}. \tag{14}$$

Noting that $uv(u-v) \equiv 0 \pmod 2$, applying Lemma 1 to (14), we complete the proof of Theorem 3.

Proof of Corollary 6. By Theorem 3, we only need to consider the case $p=3$, $q \equiv 2 \pmod 3$. Furthermore, from (14) we may assume that $3 \nmid uv(u-v)$.

If $u \equiv 1 \pmod 3$, $v \equiv 2 \pmod 3$, then

$$3 \Big| \binom{3u}{3v},$$

since $[3u/3^2] - [3v/3^2] - [3(u-v)/3^2] = 1$.

If $u \equiv 2 \pmod 3$, $v \equiv 1 \pmod 3$, then

$$3 \Big| \binom{uq}{vq},$$

since $[uq/3] - [vq/3] - [(u-v)q/3] = 1$.

Acknowledgements. The author is grateful to Professor Andrew Granville for his valuable suggestions and encouragement. Thanks are also due to the referee for his constructive report.

References

[1] T. X. Cai and A. Granville, *On the residue of binomial coefficients and their products modulo prime powers*, Acta Math. Sinica 18 (2002), 277–288.

[2] G. Eisenstein, *Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden*, Bericht. K. Pruss. Akad. Wiss. 1850, 36–42; see also G. Eisenstein, *Mathematische Werke*, Vol. II, Chelsea, 1975, 705–711.

[3] J. W. L. Glaisher, Quart. J. Math. 32 (1901), 271–305.

[4] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. 39 (1938), 350–359.

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

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

[7] —, *The New Book of Prime Number Records*, 3rd ed., Springer, 1996.

[8] J. Szmidt, J. Urbanowicz and D. Zagier, *Congruences among generalized Bernoulli numbers*, Acta Arith. 71 (1995), 273–278.

Department of Mathematics
Zhejiang University
Hangzhou, 310028, P.R. China
E-mail: txcai@mail.hz.zj.cn

Received on 13.3.2000
and in revised form on 2.2.2002 (3777)