CONGRUENCES INVOLVING EULER NUMBERS AND POWER SUMS

RICHARD J. MCINTOSH

In memory of Emma Lehmer

Abstract. In her 1938 paper on congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Emma Lehmer expresses the residues modulo prime powers of many power sums in terms of Bernoulli numbers and sometimes Euler numbers. The Euler numbers often appear in the residues of alternating power sums. In this paper, we give a new congruence for determining the residues of Euler numbers modulo a prime p. This congruence involves about $p/6$ summands of an alternating power sum. Evaluating sums of reciprocal squares modulo p, we found that there are eight Euler irregular pairs $(p, p-3)$ with $p < 5 \times 10^9$.

1. Introduction

Let p be an odd prime and k a positive integer. The congruence

$$\sum_{r=1}^{(p-1)/2} (-1)^r r^{2k} \equiv \frac{(-1)^{(p-1)/2}}{2^{2k+1}} E_{2k} \pmod{p^2} \tag{1.1}$$

can be used to determine the Euler number $E_{2k} \pmod{p^2}$. If $p-1 \nmid 2k$, then the residue of E_{2k} $\pmod p$ can be calculated using Glaisher's congruence [7, eq. (20)]

$$\sum_{r=1}^{\lfloor p/4 \rfloor} r^{2k} \equiv \frac{(-1)^{(p-1)/2}}{2^{4k+2}} E_{2k} \pmod{p}, \tag{1.2}$$

where $\lfloor p/4 \rfloor$ denotes the greatest integer not exceeding $p/4$. A slightly more efficient formula, discovered by the author in 2010, for calculating $E_{2k} \pmod p$ for $p \geq 5$ is

$$\sum_{r=1}^{\lfloor p/6 \rfloor} (-1)^r r^{2k} \equiv \frac{(-1)^{(p-1)/2}(3^{2k}+1)}{4 \cdot 6^{2k}} E_{2k} \pmod{p}, \tag{1.3}$$

provided that $3^{2k} + 1 \not\equiv 0 \pmod p$.

In her 1938 paper, Emma Lehmer [7] proved many congruences involving Bernoulli numbers and power sums. Some of her congruences also involve Euler numbers. Since that time, many papers on congruences for various power sums involving Bernoulli and Euler numbers have been written. A paper by Zhi-Hong Sun [13] extends the work of Emma Lehmer. Congruence (1.3) appears to be new. In this article, we will prove (1.3) and give an extension modulo p^3.

Emma Lehmer [7, eq. (18)], proved that for odd primes p and positive integers k, with $2k \not\equiv 2 \pmod{p-1}$,

$$\sum_{r=1}^{(p-1)/2} r^{2k} \equiv -p \frac{2^{2k-1}-1}{2^{2k}} B_{2k} \pmod{p^3},$$

where B_n is the nth Bernoulli number. When $2k \equiv 2 \pmod{p-1}$, the congruence holds modulo p^2. By [7, eq. (9)], it follows that for $p > 3$,

$$\sum_{r=1}^{\lfloor p/4 \rfloor} r^{2k} \equiv \frac{(-1)^{(p-1)/2}}{2^{4k+2}} E_{2k} - p\frac{2^{2k-1}-1}{2^{4k+1}} B_{2k} \pmod{p^2}.$$

(Modulo p, this reduces to Glaisher's congruence (1.2).) Hence,

$$\begin{aligned}\sum_{r=1}^{(p-1)/2} (-1)^r r^{2k} &= -\sum_{r=1}^{(p-1)/2} r^{2k} + 2\sum_{r=1}^{\lfloor p/4 \rfloor} (2r)^{2k} = -\sum_{r=1}^{(p-1)/2} r^{2k} + 2^{2k+1}\sum_{r=1}^{\lfloor p/4 \rfloor} r^{2k} \\ &\equiv \frac{(-1)^{(p-1)/2}}{2^{2k+1}} E_{2k} \pmod{p^2},\end{aligned}$$

which is (1.1). This congruence holds for all odd primes p and positive integers k.

2. Definitions and Formulas

The Euler polynomials $E_n(x)$ are defined by the generating function

$$\frac{2e^{xt}}{e^t+1} = \sum_{n=0}^{\infty} E_n(x)\frac{t^n}{n!}, \qquad |t| < \pi,$$

and the nth Euler number is given by $E_n = 2^n E_n(1/2)$. Thus,

$$\operatorname{sech} t = \frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} E_n \frac{t^n}{n!}, \qquad |t| < \frac{\pi}{2}.$$

There are many properties satisfied by the Euler numbers and Euler polynomials. (For a list of these properties, see [12], [1, pp. 804–806].) All Euler numbers are integers and $E_k = 0$ for all odd k. For positive even integers k, $E_k(0) = 0$. The coefficients of the Euler polynomials are rational numbers whose denominators are powers of 2. It is well known that power sums can be evaluated using Bernoulli polynomials and alternating power sums can be evaluated using Euler polynomials. In particular, for $m, k \geq 1$,

$$\sum_{r=1}^{m} (-1)^r r^k = \frac{E_k(0) + (-1)^m E_k(m+1)}{2}.$$

Because $E_{2k}(0) = 0$ for $k > 0$, it follows that

$$\sum_{r=1}^{m} (-1)^r r^{2k} = \frac{(-1)^m}{2} E_{2k}(m+1)$$

for $m, k \geq 1$. The reason why the sum in (1.3) can be used to evaluate $E_{2k} \pmod p$ is because the Euler polynomial $E_{2k}(x)$ at $x = 1/6$ is related to the value of the Euler number E_{2k} by the formula

$$2 \cdot 6^{2k} E_{2k}(1/6) = (3^{2k} + 1)E_{2k}, \qquad k \geq 0,$$

proved by equating coefficients in the power series expansion of

$$\frac{2e^x}{e^{6x}+1} + \frac{2e^{-x}}{e^{-6x}+1} = \frac{2}{e^{3x}+e^{-3x}} + \frac{2}{e^x+e^{-x}}$$

or as the special case ($n = 2k$, $m = 3$, $x = 1/6$) of the general multiplication formula

$$E_n(mx) = m^n \sum_{j=0}^{m-1} (-1)^j E_n(x + j/m)$$

for $n \geq 0$ and odd $m \geq 1$. Therefore,

$$E_{2k}\left(\frac{5}{6}\right) = E_{2k}\left(\frac{1}{6}\right) = \frac{3^{2k}+1}{2 \cdot 6^{2k}} E_{2k}$$

for $k \geq 0$, where the first equality follows from the symmetry formula

$$E_n(1-x) = (-1)^n E_n(x).$$

3. Proof of Main Result

In addition to the above identities, we will use the expansion formula

$$E_n(x+h) = \sum_{j=0}^{n} \binom{n}{j} E_{n-j}(x) h^j.$$

For prime $p \geq 5$, let $\epsilon = 1$, if $p \equiv 5 \pmod 6$ and $\epsilon = 5$, if $p \equiv 1 \pmod 6$. Then,

$$\begin{aligned}
\sum_{r=1}^{\lfloor p/6 \rfloor} (-1)^r r^{2k} &= \frac{(-1)^{\lfloor p/6 \rfloor}}{2} E_{2k}(\lfloor p/6 \rfloor + 1) \\
&= \frac{(-1)^{(p-1)/2}}{2} E_{2k}(\lfloor p/6 \rfloor + 1) \\
&= \frac{(-1)^{(p-1)/2}}{2} E_{2k}\left(\frac{p+\epsilon}{6}\right) \\
&= \frac{(-1)^{(p-1)/2}}{2} \sum_{j=0}^{2k} \binom{2k}{j} \left(\frac{p}{6}\right)^j E_{2k-j}\left(\frac{\epsilon}{6}\right) \\
&\equiv \frac{(-1)^{(p-1)/2}}{2} E_{2k}\left(\frac{\epsilon}{6}\right) \\
&= \frac{(-1)^{(p-1)/2}(3^{2k}+1)}{4 \cdot 6^{2k}} E_{2k} \pmod p,
\end{aligned}$$

which completes the proof of (1.3).

4. Euler Irregular Pairs

Vandiver [14] proved that the first case of Fermat's Last Theorem holds for a prime exponent p, if p does not divide any of the Euler numbers E_{2k} with $0 < 2k < p-1$. Such primes are called Euler regular. For prime p and $0 < 2k < p-1$, the pair $(p, 2k)$ is called an Euler irregular pair if $p | E_{2k}$. By (1.2), it follows that $(p, 2k)$ is an Euler irregular pair if p is prime, $0 < 2k < p-1$, and

$$\sum_{r=1}^{\lfloor p/4 \rfloor} r^{2k} \equiv 0 \pmod p.$$

From (1.3), we obtain the slightly more efficient test

$$\sum_{r=1}^{\lfloor p/6\rfloor}(-1)^r r^{2k}\equiv 0 \pmod p$$

for the Euler irregularity of the pair $(p, 2k)$, provided that $3^{2k}+1\not\equiv 0 \pmod p$.

By Fermat's Little Theorem, the pair $(p, p-3)$, with $p > 5$, is Euler irregular if either of the sums

$$\sum_{r=1}^{\lfloor p/4\rfloor}\frac{1}{r^2} \qquad \text{or} \qquad \sum_{r=1}^{\lfloor p/6\rfloor}\frac{(-1)^r}{r^2}$$

vanish modulo p. For $p < 5\times 10^9$, it is known that $(p, p-3)$ is an Euler irregular pair if p is equal to 149, 241, 2946901, 16467631, 17613227, 327784727, 426369739, or 1062232319. The first two were found in [5], the next three were discovered by Cosgrave and Dilcher [3] (Meštrović [10] also discovered the third prime in our list), and the last three were discovered by the author in 2012 (and are listed in [3]).

In our search for Wolstenhome primes [9, pp. 2092–2093], we used a program written by Montgomery [11] that evaluates the least two significant coefficients c_0 and $c_1 \pmod p$ in the polynomial

$$f(x)=\prod_{p/6<r<p/4}(x+r^3)$$

by use of a polynomial scheme similar to the one developed in [4, p. 441]. The sum (mod p) of the reciprocals of the roots of $f(x)$ is given by $-c_1/c_0$. The value $c_1 = 0$ would signify a Wolstenholme prime. To search for Euler irregular pairs $(p, p-3)$, we modified this program and replaced the above polynomial by

$$g(x)=\prod_{0<r<p/4}(x+r^2).$$

The conguence

$$\sum_{r=1}^{\lfloor p/6\rfloor}\frac{(-1)^r}{r^2}\equiv 0 \pmod p$$

was used (with MAPLE) to verify all Euler irregular pairs $(p, p-3)$ found by our program.

Bernoulli irregular pairs are defined in the same way as Euler irregular pairs, but with the divisibility condition $B_{2k}\equiv 0 \pmod p$. The term irregular usually refers to Bernoulli irregular. It turns out that the pair $(p, p-3)$ is (Bernoulli) irregular if and only if p is a Wolstenholme prime [8], [9]. A Wolstenholme prime is a prime p satisfying

$$\binom{2p-1}{p-1}\equiv 1 \,(\text{mod } p^4).$$

For $p\geq 11$, this is equivalent to

$$\sum_{p/6<k<p/4}\frac{1}{k^3}\equiv 0 \pmod p.$$

The only Wolstenholme primes $p < 10^{10}$ are 16843 and 2124679. The first was found (although not explicitly reported) by Selfridge and Pollak (Notices AMS **11** (1964), 97), and later confirmed by W. Johnson [6] and S. S. Wagstaff (Notices AMS **23** (1976), A-53). The second was found by J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä [2], and later, independently, by the author.

5. Concluding Remarks

Much of Lehmer's work follows from her equation [7, eq. (2)]

$$\sum_{r=1}^{\lfloor p/n\rfloor}(p-rn)^k=\frac{n^k}{k+1}\left\{B_{k+1}\left(\frac{p}{n}\right)-B_{k+1}\left(\frac{s}{n}\right)\right\},$$

where n and p are positive integers with $n<p$, and s is the least nonnegative residue of p modulo n. (A printing error in the original congruence has been corrected.) The analogous equation for alternating sums is

$$\sum_{r=1}^{\lfloor p/n\rfloor}(-1)^r(p-rn)^k=\frac{n^k}{2}\left\{(-1)^{\lfloor p/n\rfloor}E_k\left(\frac{s}{n}\right)-E_k\left(\frac{p}{n}\right)\right\}.$$

Lehmer [7, eq. (20)] proved that for odd primes p and positive integers k, with $2k\not\equiv 2 \pmod{p-1}$,

$$\sum_{r=1}^{\lfloor p/4\rfloor}(p-4r)^{2k}\equiv(-1)^{(p-1)/2}\frac{E_{2k}}{4}+p2^{4k-2}B_{2k} \pmod{p^3}.$$

When $2k\equiv 2 \pmod{p-1}$, the congruence holds modulo p^2. Using similar methods, we can show that for odd primes p and positive integers k, with $2k\not\equiv 2 \pmod{p-1}$,

$$\sum_{r=1}^{\lfloor p/6\rfloor}(-1)^r(p-6r)^{2k}\equiv(-1)^{(p-1)/2}(3^{2k}+1)\frac{E_{2k}}{4}+p6^{2k-1}(2^{2k}-1)B_{2k} \pmod{p^3}.$$

When $2k\equiv 2 \pmod{p-1}$, the congruence holds modulo p^2.

Acknowledgement. The author is grateful for the support received by the late Emma Lehmer (1906–2007) through her correspondence and discussions at the West Coast Number Theory Conference.

References

[1] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, National Bureau of Standards, 1964.

[2] J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä, *Irregular primes and cyclotomic invariants to four million*, Math. Comp., **61** (1993), 151–153.

[3] J. B. Cosgrave and K. Dilcher, *On a congruence of Emma Lehmer related to Euler numbers*, Acta Arith., **161.1** (2013), 47–67.

[4] R. E. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp., **66** (1997), 433–449.

[5] R. Ernvall and T. Metsänkylä, *Cyclotomic invariants and E-irregular primes*, Math. Comp., **32** (1978), 617–629.

[6] W. Johnson, *Irregular primes and cyclotomic invariants*, Math. Comp., **29** (1975), 113–120.

[7] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Annals of Math., **39** (1938), 350–360.

[8] R. J. McIntosh, *On the converse of Wolstenholme's Theorem*, Acta Arith., **71** (1995), 381–389.

[9] R. J. McIntosh and E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp., **76** (2007), 2087–2094.

[10] R. Meštrović, *A search for primes p such that the Euler number E_{p-3} is divisible by p*, Math. Comp., **83.290** (2014), 2967–2976.

[11] P. L. Montgomery, private communication, 1993.

[12] F. W. J. Olver et al., *NIST Handbook of Mathematical Functions*, Cambridge Univ. Press, New York, 2010, Online companion: `https://dlmf.nist.gov`.

[13] Z. -H. Sun, *Congruences involving Bernoulli and Euler numbers*, J. Number Theory, **128** (2008), 280–312.
[14] H. S. Vandiver, *Note on Euler number criteria for the first case of Fermat's last theorem*, Amer. J. Math., **62** (1940), 79–82.

MSC2010: 11B68, 11A07, 11A41, 11Y99

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF REGINA, REGINA, SASKATCHEWAN S4S 0A2, CANADA
Email address: Richard.Mcintosh@uregina.ca