

10-1-2010

A supercongruence motivated by the Legendre family of elliptic curves

Heng Huat Chan
National University of Singapore

Ling Long
Iowa State University

V. V. Zudilin
The University of Newcastle, Australia

Follow this and additional works at: https://digitalcommons.lsu.edu/mathematics_pubs

Recommended Citation

Chan, H., Long, L., & Zudilin, V. (2010). A supercongruence motivated by the Legendre family of elliptic curves. *Mathematical Notes*, 88 (3-4), 599-602. <https://doi.org/10.1134/S0001434610090324>

This Article is brought to you for free and open access by the Department of Mathematics at LSU Digital Commons. It has been accepted for inclusion in Faculty Publications by an authorized administrator of LSU Digital Commons. For more information, please contact ir@lsu.edu.

A SUPERCONGRUENCE MOTIVATED BY THE LEGENDRE FAMILY OF ELLIPTIC CURVES

HENG HUAT CHAN, LING LONG, AND WADIM ZUDILIN

In blessed memory of Anatoly Alekseevich Karatsuba

ABSTRACT. A new supercongruence associated with a Gaussian hypergeometric series, as well as one of Mortenson's supercongruences, are established with new congruence relations and the Legendre transforms of certain sequences.

1. INTRODUCTION

The Legendre family of elliptic curves

$$E_a : y^2 = x(x-1)(x-a)$$

is well known in the literature. For any fixed complex number a , E_a corresponds to a double cover of the complex line ramified at four points: 0 , 1 , a , and ∞ . If a is different from 0 , 1 , ∞ , the resulting covering curve is an elliptic curve, topologically isomorphic to a torus. Elliptic curve is a well-studied subject and has many important applications such as the Elliptic Curve Cryptography.

Let p be an odd prime and a be p -integral not equal to 0 or 1 . Let $\#(E_a/\mathbf{F}_p)$ be the number of solutions E_a over the finite field \mathbf{F}_p . From the computations of the Hasse invariant of the elliptic curve E_a [7, Chapter V, Section 4], it is known that

$$\#(E_a/\mathbf{F}_p) \equiv - \sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-4k} a^k \pmod{p}. \quad (1)$$

We mention here that the upper limit of the original sum is $p-1$. However, we may replace $p-1$ by $(p-1)/2$ since for $k \geq (p+1)/2$,

$$\binom{2k}{k} \equiv 0 \pmod{p}.$$

On the other hand, from [2, Sections 2.8–2.11] we know that

$$\#(E_a/\mathbf{F}_p) \equiv - \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 a^k \pmod{p}. \quad (2)$$

Combining (1) and (2), we conclude that

$$\sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-4k} a^k \equiv \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 a^k \pmod{p}. \quad (3)$$

The first author was supported by NUS Academic Research Grant R-146-000-103-112. The second author was supported by NSA grant H98230-08-1-0076.

The congruence (3) can be proved directly by observing that

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

Now, when $a = 2$, the elliptic curve has the so-called complex multiplication. Roughly speaking, this means E_2 admits extra symmetries. For instance, if (x, y) is a pair of solution E_2 then $(-x + 2, \sqrt{-1} \cdot y)$ is another. It is known that E_2 is supersingular over \mathbf{F}_p when $p \equiv 3 \pmod{4}$ (see [7, §V.4] for definition). Therefore, by the proof of Theorem 4.1 [7, §V.4], if $p \equiv 3 \pmod{4}$ then

$$\#(E_a/\mathbf{F}_p) \equiv 0 \pmod{p}. \quad (5)$$

Hence, we have the following “modified” version of (3):

$$\sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-3k} \equiv (-1)^{(p-1)/2} \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 2^k \pmod{p}, \quad (6)$$

with the factor $(-1)^{(p-1)/2}$ inserted.

It turns out that the following supercongruence is true:

Theorem 1. *Let $p \equiv 1 \pmod{2}$ be a prime, and $n = (p-1)/2$. Then*

$$\sum_{k=0}^n \binom{2k}{k}^2 2^{-3k} \equiv (-1)^n \sum_{k=0}^n \binom{n}{k}^2 2^k \pmod{p^2}. \quad (7)$$

Our aim of this short note is to prove (7). The surprising fact is that although most proofs of “supercongruences” involve methods like the Wilf–Zeilberger algorithm (see [6], [8]), Gaussian hypergeometric series (such as [1], [6]), hypergeometric series evaluation identities (see, for example, [3]), the proof of (7) requires only some elementary binomial identities.

2. PROOF OF THEOREM 1

The proof of Theorem 1 follows from two simple lemmas.

Lemma 1. *Let p be a prime and $n = (p-1)/2$; then*

$$\sum_{k=0}^n (-2)^k \binom{n}{k} \binom{n+k}{k} \equiv \sum_{k=0}^n \binom{2k}{k}^2 2^{-3k} \pmod{p^2}. \quad (8)$$

Proof. Note that

$$\begin{aligned} \frac{(\frac{1}{2} + \varepsilon)_k}{k!} &= \frac{(\frac{1}{2} + \varepsilon)(\frac{1}{2} + \varepsilon + 1) \cdots (\frac{1}{2} + \varepsilon + k - 1)}{k!} \\ &= \frac{(\frac{1}{2})_k}{k!} \left(1 + 2\varepsilon \sum_{j=1}^k \frac{1}{2j-1} + O(\varepsilon^2) \right). \end{aligned} \quad (9)$$

Substituting $\varepsilon = p/2$ and $\varepsilon = -p/2$ in (9), we find that

$$\binom{n+k}{k} = \frac{(\frac{1}{2})_k}{k!} \left(1 + p \sum_{j=1}^k \frac{1}{2j-1} + O(p^2) \right)$$

and

$$(-1)^k \binom{n}{k} = \frac{\left(\frac{1}{2}\right)_k}{k!} \left(1 - p \sum_{j=1}^k \frac{1}{2j-1} + O(p^2)\right),$$

respectively. Therefore,

$$(-1)^k \binom{n}{k} \binom{n+k}{k} = \left(\frac{\left(\frac{1}{2}\right)_k}{k!}\right)^2 (1 + O(p^2)). \quad (10)$$

After multiplication by 2^k and summing everything up, we arrive at (8). \square

The *Legendre transform* of a sequence $\{c_k\}_{k=0}^{\infty}$ is the sequence $\{a_n\}_{n=0}^{\infty}$ that satisfies the relation

$$a_n = \sum_{k=0}^n \binom{n+k}{k} \binom{n}{k} c_k, \quad n = 0, 1, 2, \dots$$

To complete the proof of Theorem 1, we will find the Legendre transform of the sequence $(-2)^k$.

Lemma 2. *The following is true for any non-negative integer n :*

$$\sum_{k=0}^n (-2)^k \binom{n}{k} \binom{n+k}{k} = (-1)^n \sum_{k=0}^n \binom{n}{k}^2 2^k. \quad (11)$$

Proof. Write

$$\binom{n+k}{k} = \sum_{j=0}^k \binom{n}{j} \binom{k}{k-j}.$$

Then

$$\begin{aligned} \sum_{k=0}^n (-2)^k \binom{n}{k} \binom{n+k}{k} &= \sum_{k=0}^n (-2)^k \binom{n}{k} \sum_{j=0}^k \binom{n}{j} \binom{k}{k-j} \\ &= \sum_{j=0}^n \binom{n}{j} \sum_{k=j}^n (-2)^k \binom{n}{k} \binom{k}{k-j} \\ &= \sum_{j=0}^n \binom{n}{j}^2 \sum_{k=j}^n (-2)^k \binom{n-j}{k-j}, \end{aligned}$$

since

$$\binom{n}{k} \binom{k}{k-j} = \binom{n}{j} \binom{n-j}{k-j}.$$

Therefore,

$$\begin{aligned} \sum_{k=0}^n (-2)^k \binom{n}{k} \binom{n+k}{k} &= \sum_{j=0}^n \binom{n}{j}^2 \sum_{l=0}^{n-j} (-2)^{l+j} \binom{n-j}{l} \\ &= \sum_{j=0}^n \binom{n}{j}^2 (-2)^j \sum_{l=0}^{n-j} (-2)^l \binom{n-j}{l} \\ &= \sum_{j=0}^n \binom{n}{j}^2 (-2)^j (-1)^{n-j} = (-1)^n \sum_{j=0}^n \binom{n}{j}^2 2^j. \quad \square \end{aligned}$$

The proof of Theorem 1 now follows from (8) and (11).

As a corollary of Theorem 1, we see that the congruence (5) holds.

Remark. In the case $a = 1$, the cubic equation $y^2 = x(x - 1)^2$ is singular, that is, the curve E_1 is isomorphic to a sphere but not a torus. This is the degenerate case corresponding to a related supercongruence,

$$\sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-4k} \equiv (-1)^{(p-1)/2} \pmod{p^2}, \quad (12)$$

due to Mortenson [4, Theorem 1] (see also [5, Eq. (1.1)]). It can be also shown using the elementary ideas in the proofs of Lemmas 1 and 2.

Indeed, summing (10) over k we conclude that

$$\sum_{k=0}^{(p-1)/2} \binom{n}{k} \binom{n+k}{k} (-1)^k \equiv \sum_{k=0}^{(p-1)/2} \binom{2k}{k}^2 2^{-4k} \pmod{p^2}. \quad (13)$$

On the other hand, it is not difficult to see that

$$\sum_{k=0}^n \binom{n}{k} \binom{n+k}{k} (-1)^k = (-1)^n. \quad (14)$$

Combining (13) and (14), we arrive at the congruence (12).

It would be nice to have similar elementary proofs for other Mortenson's supercongruences [5, Eqs. (1.2)–(1.4)].

Acknowledgements. The authors would like to thank Robert Osburn, whose conversation with the second author inspired our discovery, and Eric Mortenson for valuable comments. The first and second authors would like to thank National Center for Theoretical Sciences in Hsinchu Taiwan, where the project was started. Also the work was carried out whilst the first author was visiting in the Max Planck Institute for Mathematics (MPIM). He thanks the MPIM for providing a nice research environment.

REFERENCES

- [1] S. AHLGREN and K. ONO, A Gaussian hypergeometric series evaluation and Apéry number congruences, *J. Reine Angew. Math.* **518** (2000), 187–212.
- [2] C. H. CLEMENS, *A scrapbook of complex curve theory*, University Series in Math. (Plenum Press, New York, 1980).
- [3] D. MCCARTHY and R. OSBURN, A p -adic analogue of a formula of Ramanujan, *Arch. Math. (Basel)* **91**:6 (2008), 492–504.
- [4] E. MORTENSON, A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function, *J. Number Theory* **99** (2003), 139–147.
- [5] E. MORTENSON, Supercongruences between truncated ${}_2F_1$ hypergeometric functions and their Gaussian analogs, *Trans. Amer. Math. Soc.* **355**:3 (2003), 987–1007.
- [6] R. OSBURN and C. SCHNEIDER, Gaussian hypergeometric series and supercongruences, *Math. Comput.* **78** (2009), 275–292.
- [7] J. H. SILVERMAN, *The arithmetic of elliptic curves* (Springer-Verlag, New York, 1986).
- [8] W. ZUDILIN, Ramanujan-type supercongruences, *J. Number Theory* **129**:8 (2009), 1848–1857.

DEPARTMENT OF MATHEMATICS, NATIONAL UNIVERSITY OF SINGAPORE, 2 SCIENCE DRIVE
2, SINGAPORE 117543

E-mail address: `matchh@nus.edu.sg`

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IA 50011 USA

E-mail address: `linglong@iastate.edu`

SCHOOL OF MATHEMATICAL AND PHYSICAL SCIENCES, UNIVERSITY OF NEWCASTLE, CALLAGHAN
NSW 2308, AUSTRALIA

E-mail address: `wadim.zudilin@newcastle.edu.au`