ISSN 0001-4346, Mathematical Notes, 2010, Vol. 88, No. 4, pp. 599–602. © Pleiades Publishing, Ltd., 2010.
Published in Russian in Matematicheskie Zametki, 2010, Vol. 88, No. 4, pp. 620–624.

A Supercongruence Motivated by the Legendre Family of Elliptic Curves*

Heng Huat Chan[1], Ling Long[2***], and V. V. Zudilin[3****]**

[1] *National University of Singapore, Singapore*
[2] *Iowa State University, USA*
[3] *University of Newcastle, Australia*

Received January 24, 2010

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.

DOI: 10.1134/S0001434610090324

Key words: *elliptic curve, ramified double cover, finite field, Hasse invariant, supercongruence, Legendre transform.*

In blessed memory of Anatolii Alekseevich Karatsuba

1. INTRODUCTION

The Legendre family of elliptic curves

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

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 curves constitute a well-studied subject and have many important applications, such as Elliptic-Curve Cryptography.

Let p be an odd prime and a be p-integral, $a \neq 0, 1$. 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 [1, Chap. V, Sec. 4], it is known that

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

We mention here that the upper limit of the original sum was $p-1$. 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, Secs. 2.8—2.11], we know that

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

*The text was submitted by the authors in English.

**E-mail: matchh@nus.edu.sg
***E-mail: linglong@iastate.edu
****E-mail: wadim.zudilin@newcastle.edu.au

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

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

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

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

Now, when $a = 2$, the so-called complex multiplication is defined on the elliptic curve. 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 [1, Sec. V.4] for the definition). Therefore, by the proof of Theorem 4.1 in [1, Sec. V.4], if $p \equiv 3 \pmod 4$, then

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

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

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

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

It turns out that the following supercongruence is true:

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

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

Our aim in 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 [3], [4]), Gaussian hypergeometric series (as in, e.g., [5], [3]), hypergeometric series evaluation identities (see, e.g., [6]), 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*

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

Proof. Note that

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

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

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

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

respectively. Therefore,

$$(-1)^k\binom{n}{k}\binom{n+k}{k}=\biggl(\frac{(1/2)_k}{k!}\biggr)^2\bigl(1+O(p^2)\bigr). \tag{10}$$

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

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

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

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 nonnegative integer* n:

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

Proof. Write

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

Then

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

because

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

Therefore,

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

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 1. 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 to a torus. This is the degenerate case corresponding to a related supercongruence,

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

due to Mortenson [7, Theorem 1] (see also [8, (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

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

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

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

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

It would be nice to have similar elementary proofs for Mortenson's other supercongruences [8, (1.2)–(1.4)].

ACKNOWLEDGMENTS

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 the 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.

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.

REFERENCES

1. J. H. Silverman, *The Arithmetic of Elliptic Curves*, in *Grad. Texts in Math.* (Springer-Verlag, New York, 1986), Vol. 106.
2. C. H. Clemens, *A Scrapbook of Complex Curve Theory*, in *Univ. Ser. Math.* (Plenum Press, New York, 1980).
3. R. Osburn and C. Schneider, "Gaussian hypergeometric series and supercongruences," Math. Comp. **78** (265), 275–292 (2009).
4. W. Zudilin, "Ramanujan-type supercongruences," J. Number Theory **129** (8), 1848–1857 (2009).
5. S. Ahlgren and K. Ono, "A Gaussian hypergeometric series evaluation and Apéry number congruences," J. Reine Angew. Math. **518**, 187–212 (2000).
6. D. McCarthy and R. Osburn, "A p-adic analogue of a formula of Ramanujan," Arch. Math. (Basel) **91** (6), 492–504 (2008).
7. E. Mortenson, "A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function," J. Number Theory **99** (1), 139–147 (2003).
8. E. Mortenson, "Supercongruences between truncated ${}_2F_1$ hypergeometric functions and their Gaussian analogs," Trans. Amer. Math. Soc. **355** (3), 987–1007 (2003).