J. Math. Soc. Japan
Vol. 64, No. 1 (2012) pp. 87–89
doi: 10.2969/jmsj/06410087

Erratum to "The cuspidal class number formula for the modular curves $X_1(2p)$"

[The original paper is in this journal, Vol. 64 (2012), 23–85]

By Toshikazu Takagi

(Received May 26, 2011)

Abstract. We correct a theorem on the conductor of elliptic curves over $\boldsymbol{Q}$ given in Introduction of the paper "The cuspidal class number formula for the modular curves $X_1(2p)$".

In Introduction of Takagi [**3**], I gave a theorem concerning the conductor of elliptic curves over $\boldsymbol{Q}$. But, since our arguments contained an error, the statement of the theorem had a surplus assumption in the case of the prime conductor. I give the corrected statement in the following.

Let A be an elliptic curve over $\boldsymbol{Q}$ of conductor n. Let r be 5 or 7 with $r \nmid n$. Agashe [**1**] proved that if n is square-free and r divides the order of the $\boldsymbol{Q}$-rational torsion subgroup of $A(\boldsymbol{Q})$, then r divides the cuspidal class number $h_0(n)$ of $X_0(n)$.

When n is a prime, Ogg [**6**] has shown that $h_0(n)$ is equal to the numerator of $(n-1)/12$. On the other hand, in Takagi [**2**, Theorem 5.1], we gave the cuspidal class number formula for n square-free, generalizing the formula of Ogg. When n is composite, we see from this that r divides $h_0(n)$ if and only if n has a prime factor congruent to ± 1 modulo r. Combining these results we have the following

Theorem. *Let n be a square-free integer. Let A be an elliptic curve over $\boldsymbol{Q}$ of conductor n. Let r be 5 or 7 with $r \nmid n$.*

(1) *Assume that n is a prime. If A has a $\boldsymbol{Q}$-rational point of order r, then $n \equiv 1 \pmod{r}$.*
(2) *Assume that n is composite. If A has a $\boldsymbol{Q}$-rational point of order r, then n has a prime factor congruent to ± 1 modulo r.*

Examples. In Table 1 of Cremona [**4**], all elliptic curves over $\boldsymbol{Q}$ of conductor $n \leqq 1000$ are listed. In the list there exist 45 elliptic curves A with $5 \mid |A(\boldsymbol{Q})|$.

2010 *Mathematics Subject Classification.* Primary 11G18; Secondary 11F03, 11G05, 14G05, 14G35, 14H40, 14H52.

Key Words and Phrases. modular curve, modular unit, cuspidal class number, elliptic curve, Jacobian variety, torsion subgroup.

Among them the number of the curves with $5 \nmid n$ is 25, and all these 25 curves have a square-free conductor. Among the 25 curves, the number of the curves such that n is a prime is 2, and both of them (the curves 11A1 and 11A3) have the conductor $n = 11 \equiv 1 \pmod 5$, which are examples of the case (1) of the theorem. Among the other 23 curves which have a composite n, the number of the curves such that n has a prime factor p with $p \equiv 1 \pmod 5$ (respectively $p \equiv -1 \pmod 5$) is 14 (respectively 9). The curves with the least n which have a prime factor $p \equiv 1 \pmod 5$ are 66C1 and 66C2. Both of them have the conductor $n = 66 = 2 \cdot 3 \cdot 11$ with $p = 11$. The curve with the least n which have a prime factor $p \equiv -1 \pmod 5$ is 38B1, and its conductor is $n = 38 = 2 \cdot 19$ with $p = 19$.

In the list there exist 10 elliptic curves A with $7 \mid |A(\boldsymbol{Q})|$. Among them the number of the curves with $7 \nmid n$ is 6, and all these 6 curves have a composite, square-free conductor. Among the 6 curves, the number of the curves such that n has a prime factor p with $p \equiv 1 \pmod 7$ (respectively $p \equiv -1 \pmod 7$) is 4 (respectively 2). The curve with the least n which has a prime factor $p \equiv 1 \pmod 7$ is 174B1, and its conductor is $n = 174 = 2 \cdot 3 \cdot 29$ with $p = 29 \equiv 1 \pmod 7$. The curve with the least n which has a prime factor $p \equiv -1 \pmod 7$ is 26B1, and its conductor is $n = 26 = 2 \cdot 13$ with $p = 13 \equiv -1 \pmod 7$.

Observations. The theorem considers the elliptic curves of conductor n with $r \nmid n$. On the contrary, for the elliptic curves of conductor n with $r \mid n$, we have the following observations. In Table 1 of Cremona [**5**], all elliptic curves over $\boldsymbol{Q}$ of conductor $n < 180000$ are listed. In the list there exist 868 (respectively 54) elliptic curves A with $5 \mid |A(\boldsymbol{Q})|$ (respectively $7 \mid |A(\boldsymbol{Q})|$), among them the number of the curves such that $5 \mid n$ (respectively $7 \mid n$) is 456 (respectively 21), and the number of the curves such that $5 \parallel n$ (respectively $7 \parallel n$) is 283 (respectively 12). For each $r = 5, 7$, we observe that all curves in this list with $r \mid |A(\boldsymbol{Q})|$ and $r \parallel n$ satisfy that the conductor n is square-free and has a prime factor congruent to ± 1 modulo r.

References

[1] A. Agashe, Rational torsion in elliptic curves and the cuspidal subgroup, preprint, arXiv:math/0810.5181, 2008.

[2] T. Takagi, The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free, J. Algebra, **193** (1997), 180–213.

[3] T. Takagi, The cuspidal class number formula for the modular curves $X_1(2p)$, J. Math. Soc. Japan, **64** (2012), 23–85.

[4] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge Univ. Press, Cambridge, second edition, 1997.

[5] J. E. Cremona, Elliptic curve data (updated 2011-08-09), http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html

[6] A. Ogg, Rational points on certain elliptic modular curves, In: Analytic Number Theory,

Proc. Sympos. Pure Math., **XXIV**, St. Louis Univ. St. Louis, 1972, Amer. Math. Soc., Providence, RI, 1973, pp. 221–231.

Toshikazu Takagi
Faculty of Arts and Sciences at Fujiyoshida
Showa University
Fujiyoshida
Yamanashi 403-0005, Japan
E-mail: takagi@cas.showa-u.ac.jp