Commun. Korean Math. Soc. **22** (2007), No. 2, pp. 207–208

CORRIGENDUM ON "THE NUMBER OF POINTS ON ELLIPTIC CURVES $E : y^2 = x^3 + cx$ OVER $\mathbb{F}_p$ MOD 8"

İLKER İNAM, GÖKHAN SOYDAN, MUSA DEMIRCI, OSMAN BIZIM, AND İSMAIL NACI CANGÜL

ABSTRACT. In this work, authors considered a result concerning elliptic curves $y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8, given at [1]. They noticed that there should be a slight change at this result. They give counterexamples and the correct version of the result.

In [1] the following main theorem is given:

Theorem 1. *If $p \equiv 1, 5 (\mathrm{mod}\, 8)$ is a rational prime then*

$$\#E = \begin{cases} 0 \pmod 8 & \text{if c is a quartic residue in } \mathbb{F}_p, \\ 4 \pmod 8 & \text{if c is a quadratic residue but quartic non} - \text{residue in } \mathbb{F}_p, \\ 2 \pmod 8 & \text{if c is a quadratic non} - \text{residue in } \mathbb{F}_p. \end{cases}$$

In our study of these elliptic curves, we noticed that the above result is true when $p \equiv 1 \pmod 8$, and needs a slight change when $p \equiv 5 \pmod 8$. Indeed, for example when $p = 29$, which is $\equiv 5 \pmod 8$, the quadratic residues which are non-quartic are $4, 5, 6, 9, 13, 22, 28$. If we take $c = 4$, that is, $y^2 = x^3 + 4x \pmod{29}$, which can also be thought of as the elliptic curve $y^2 = x^3 - 25x \pmod{29}$, by [2] this last elliptic curve has 40 rational points, and $40 \equiv 0 \pmod 8$. Note that 4 is a quadratic but non-quartic residue and by Theorem 1 one would have $\#E \equiv 4 \pmod 8$.

Similarly for the other values of c in the above list, similar results can be obtained.

For the other case in Theorem 1, let $c = 7$. Then $y^2 = x^3 + 7x \pmod{29}$ can be equivalently be thought of as $y^2 = x^3 - 22x \pmod{29}$, and again by [2] $\#E = 20 \equiv 4 \pmod 8$. But according to Theorem 1, as 7 is a quartic residue, one would have $\#E \equiv 0 \pmod 8$.

Therefore, the theorem should be as follows

Theorem 2. *If p is a rational prime, then*

Received May 17, 2006.
2000 *Mathematics Subject Classification.* 11G20, 14G05.
Key words and phrases. elliptic curves over finite fields, rational points.

when $p \equiv 1 \pmod 8$,

$$\#E = \begin{cases} 0 \pmod 8 & if\ c\ is\ a\ quartic\ residue\ in\ \mathbb{F}_p \\ 4 \pmod 8 & if\ c\ is\ a\ quadratic\ residue\ but\ quartic\ non-residue\ in\ \mathbb{F}_p \\ 2 \pmod 8 & if\ c\ is\ a\ quadratic\ non-residue\ in\ \mathbb{F}_p, \end{cases}$$

and when $p \equiv 5 \pmod 8$,

$$\#E = \begin{cases} 4 \pmod 8 & if\ c\ is\ a\ quartic\ residue\ in\ \mathbb{F}_p \\ 0 \pmod 8 & if\ c\ is\ a\ quadratic\ residue\ but\ quartic\ non-residue\ in\ \mathbb{F}_p \\ 2 \pmod 8 & if\ c\ is\ a\ quadratic\ non-residue\ in\ \mathbb{F}_p. \end{cases}$$

It seems that the authors are confused by the use of formulae (3 - 7) and (3 - 8) which are valid for $p \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$, respectively, whereas they are both used for general result.

References

[1] H. Park, D. Kim, and H. Lee, *The number of points on elliptic curves* $E : y^2 = x^3 + cx$ *over* F_p *Mod 8,* Commun. Korean Math. Soc. **18** (2003), no. 1, 31–37.

[2] M. Demirci, Y. N. İkikardeş, G. Soydan, and İ. N. Cangül, *Frey Elliptic Curves* $y^2 = x^3 - n^2x$ *on finite fields* F_p *where* $p \equiv 1\,(4)$ *is prime,* to be printed.

İLKER İNAM
DEPARTMENT OF MATHEMATICS
ULUDAĞ UNIVERSITY
16059 BURSA, TURKEY
E-mail address: inam@uludag.edu.tr

GÖKHAN SOYDAN
DEPARTMENT OF MATHEMATICS
ULUDAĞ UNIVERSITY
16059 BURSA, TURKEY
E-mail address: gsoydan@uludag.edu.tr

MUSA DEMIRCI
DEPARTMENT OF MATHEMATICS
ULUDAĞ UNIVERSITY
16059 BURSA, TURKEY
E-mail address: mdemirci@uludag.edu.tr

OSMAN BIZIM
DEPARTMENT OF MATHEMATICS
ULUDAĞ UNIVERSITY
16059 BURSA, TURKEY
E-mail address: obizim@uludag.edu.tr

İSMAIL NACI CANGÜL
DEPARTMENT OF MATHEMATICS
ULUDAĞ UNIVERSITY
16059 BURSA, TURKEY
E-mail address: cangul@uludag.edu.tr