Erratum to "Factorisation patterns of division polynomials"

By Hugues VERDURE

Institutt for matematikk og statistikk, Universitetet i Tromsø
9037 Tromsø, Norway

Key words: Elliptic curve; division polynomial; factorisation.

The statement of Propostion 2 of paper [2] is partially incorrect due to a flaw in the proof. The fourth case of the proposition should be replaced by two subcases. Simultaneously, the proof should be slightly changed in the lines 8 to 5 from the bottom of the second column of page 81 ("Finally, if R is a non-zero ... both α and β are even"). The proposition should read:

Proposition 2. *Let E be an elliptic curve defined over $\mathbf{F}_q$. Let α be the degree of the minimal extension over which E has a non-zero l-torsion point. Assume that $E[l] \not\subset E(\mathbf{F}_{q^\alpha})$. Let $\rho \in \mathbf{F}_l^*$ be as defined in Lemma* 1. *Let β be the order of $\frac{q}{\rho}$ in $\mathbf{F}_l^*$. Then the pattern of $\psi_l(x)$ is:*

$\left(\left(\alpha, \frac{l-1}{2\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha\vee\beta, \frac{(l-1)^2}{2(\alpha\vee\beta)}\right)\right)$ *if α and β are odd, and $q \neq \rho^2$,*

$\left(\left(\alpha, \frac{l-1}{2\alpha}\right), \left(\frac{\beta}{2}, \frac{l-1}{\beta}\right), \left(\alpha\vee\beta, \frac{(l-1)^2}{2(\alpha\vee\beta)}\right)\right)$ *if α is odd, β is even and $q \neq \rho^2$,*

$\left(\left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha\vee\beta, \frac{(l-1)^2}{2(\alpha\vee\beta)}\right)\right)$ *if α is even, β is odd and $q \neq \rho^2$,*

$\left(\left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\frac{\beta}{2}, \frac{l-1}{\beta}\right), \left(\frac{\alpha\vee\beta}{2}, \frac{(l-1)^2}{\alpha\vee\beta}\right)\right)$ *if α and β are even with equal 2-valuations and $q \neq \rho^2$,*

$\left(\left(\alpha, \frac{l-1}{2\alpha}\right), \left(\frac{\beta}{2}, \frac{l-1}{\beta}\right), \left(\alpha\vee\beta, \frac{(l-1)^2}{2(\alpha\vee\beta)}\right)\right)$ *if α and β are even with different 2-valuations and $q \neq \rho^2$,*

$\left(\left(\alpha, \frac{l-1}{2\alpha}\right), \left(\alpha l, \frac{l-1}{2\alpha}\right)\right)$ *if α is odd and $q = \rho^2$,*

$\left(\left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\frac{\alpha l}{2}, \frac{l-1}{\alpha}\right)\right)$ *if α is even and $q = \rho^2$.*

Proof. Replace the erroneous sentence in the original proof by: Finally, if R is any non-zero l-torsion point not of the two previous forms, then $\varphi^n(R) = -R$ is possible just in the case where both α and β are even with equal 2-valuations. In that case, n is positive minimal with that property if and only if $n = \frac{\alpha}{2} \vee \frac{\beta}{2} = \frac{\alpha\vee\beta}{2}$. In all the other cases, $\varphi^n(R) \neq -R$ for all integers n, and $\varphi^n(R) = R$ with n positive minimal if and only if $n = \alpha \vee \beta$. □

Acknowledgment. The error was pointed out via the editor by Prof. Daniel Sadornil, Dpto. Matematicas, Universidad de Salamanca, Spain. The author is sincerely thankful to Prof. Daniel Sadornil.

References

[1] Sadornil, D.: A note on factorisation of division polynomials, available at arxiv.org math.NT/0606684.

[2] Verdure, H.: Factorisation patterns of division polynomials. Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), no. 5, 79–82.

2000 Mathematics Subject Classiffcation. 14H52, 11T71