3.3.1 Division

Division will be defined as a multiplication by the inverse. For $P_{\mathcal{A}}$ and $P_{\mathcal{B}}$ shown in Eqs.(30), consider

$$P_{\mathcal{C}} = [\mathcal{C}]P = [\mathcal{A} \cdot \mathcal{B}^{-1}]P = P_{\mathcal{A}} \cdot P_{\mathcal{B}}^{-1}. \quad (36)$$

According to Itoh–Tsujii inversion algorithm [16] with Eq.(31), the inverse $\mathcal{B}^{-1}$ for $P_{\mathcal{B}}^{-1} = [\mathcal{B}^{-1}]P$ in the case of $d = 3$, for example, is given by

$$\begin{aligned}
\mathcal{B}^{-1} &= \mathcal{B}^r \cdot (\mathcal{B} \cdot \mathcal{B}^r)^{-1} \\
&= (b_0 + b_1\hat{\pi}_3) \cdot \{(b_0 + b_1\hat{\pi}_3) \cdot (b_0 + b_1\hat{\pi}_3^r))\}^{-1} \\
&= (b_0 + b_1\hat{\pi}_3) \cdot \left\{(b_0 + b_1\hat{\pi}_3) \cdot (b_0 + b_1\hat{\pi}_3^{-1}))\right\}^{-1} \\
&= (b_0 + b_1\hat{\pi}_3) \cdot \left(b_0^2 + b_1^2 - b_0b_1\right)^{-1} \\
&= w \cdot b_0 + w \cdot b_1\hat{\pi}_3, \quad (37)
\end{aligned}$$

where $w = (b_0^2 + b_1^2 - b_0b_1)^{-1} \bmod r$ and $\hat{\pi}_3^r = \hat{\pi}_3^{-1}$ modulo $f'(\hat{\pi}_3) = 0$. Thus, *division* is also available with the same manner of that of $\mathbb{F}_{r^2}$.

4 Future works

This paper has given a *multiplicative* representation of r–torsion rational points in the same manner of elemenets in the second extension field $\mathbb{F}_{r^2}$. Then, it was shown that all of r–torsion points except for the infinity $\mathcal{O}$ form a cyclic group in the same of the multiplicative group $\mathbb{F}_{r^2}^*$. As a future work, based on the approach shown in this paper, some cryptographic applications or attacks toghther with *pairing* will be given. Though this paper did not deal with, the case that period n divides order r will have some interesting properties.

References

[1] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," *SCIS 2000*, Jan. 2000.

[2] T. Nakanishi and N. Funabiki, "Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps," Asiacrypt 2005, LNCS, vol. 3788, pp. 443-454, 2005.

[3] H. Cohen and G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, *Discrete Mathematics and Its Applications*, Chapman & Hall CRC, 2005.

[4] Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, "Integer Variable χ–based Ate Pairing," *Pairing 2008*, LNCS 5209, pp. 178–191, 2008.

[5] Y. Sakemi, Y. Nogami, K. Okeya, H. Kato, and Y. Morikawa, "Skew Frobenius Map and Efficient Scalar Multiplication for Pairing–based Cryptography," *CANS 2008*, LNCS 5339, Springer–Verlag, pp. 226-239, 2008.

[6] S. D. Galbraith and M. Scott , "Exponentiation in Pairing–Friendly Groups Using Homomorphisms," *Pairing 2008*, LNCS 5209, Springer–Verlag, pp. 211–224, 2008.

[7] N. Smart, I. F. Blake, and G. Seroussi, *Elliptic Curves in Cryptography*," LMS Lecture Note Series, Cambridge University Press, 1999.

[8] S. Hirasawa and A. Miyaji, "Elliptic Curves with a Pre–determined Embedding Degree," IEICE Tech. Rep., ISEC2008–82, pp. 63–66, 2008.

[9] K. Ohta and K. Shiota, "Construction of CM Curves Suitable for Cryptosystem from the Weil Pairing," Memoirs of the Faculty of Science, Kochi Univ., Vol. 27, No. 1, 2007.

[10] L. E. Dickson, "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group," Ann. of Math., 1897.

[11] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curves Cryptography*, Springer–Verlag, 2004.

[12] D. Charles, "On the existence of distortion maps on ordinary elliptic curves," in Cryptology ePrint Archive, Report 2006/128, 2006.

[13] D. Boneh, A. Sahai, and B. Waters, "Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys," *Eurocrypt 2006*, LNCS 4004, pp. 573–592, 2006.

[14] T. Izuta, S. Takeuchi, K. Nishii, Y. Nogami, and Y. Morikawa, "GLV Subgroups on Non–supersingular Pairing–friendly Curves of Embedding Degree 1," *Computer Security Symposium 2010*, pp. 249 – 254, 2010.

[15] P. S. L. M. Barreto, and M. Naehrig, "Pairing–Friendly. Elliptic Curves of Prime Order," SAC2005, LNCS 3897, pp. 319-331, 2006.

[16] T. Itoh and S. Tsujii, "A Fast Algorithm for Computing Multiplicative Inverses in GF(2^m) Using Normal Bases," *Inf. and Comp.*, vol. 78, pp. 171–177, 1988.