1035-11-118 **Juliana V. Belding*** (jbelding@math.umd.edu), University of Maryland, College Park. *A Weil pairing on the p-torsion of ordinary elliptic curves over $K[\epsilon]$.*

For an elliptic curve E over any field K, the Weil pairing e_n is a bilinear map on n-torsion. For K of characteristic $p > 0$, the map e_n is degenerate if and only if n is divisible by p. In this paper, we consider E over the dual numbers $K[\epsilon]$ and define a non-degenerate "Weil pairing on p-torsion" which shares many of the same properties of the Weil pairing. We also show that the discrete logarithm attacks on p-torsion subgroups of Semaev and Rück may be viewed as Weil-pairing-based attacks, just like the MOV attack. Finally, we describe an attack on the discrete logarithm problem on anomalous curves, analogous to that of Smart, using a lift of E over $\mathbb{F}_p[\epsilon]$. (Received September 19, 2007)