0 Introduction

HEC are...

This paper sets out to imitate the approach and techniques used on elliptic curves in a series of lectures given by Prof. David Masser between 2009 and 2010. The aim is to define a group law on the set of solutions to $y^2 = C(x)$ where the bulk of the work will be going into proving associativity.

Behind the choice of this approach lies the desire to not only derive an explicit addition law, but also to xxx elementary without the need to delve into xxx/ use the tools from algebraic geometry

Many papers and a few books have been written about this subject

The reason for restricting ourselves to curves of genus 2 lies in the explicit nature of our group law. Whereas other bblah, we do it the other way around and give the addition law first with the definition divisors following as a result.

The reason for examining degree 5 / genus 2 is...

– The special attraction in genus 2 is ...

———

what this paper is (& is not)

motivation for this paper...

special attraction genus 2

Our approach therefore diverges from what has become the standard approach for computational uses [cite zuccherato]

—-

application ¿ crypto

the inspiration for this came from a two-part lecture on elliptic curves by Prof. David Masser in fall? of 2009. Set out to imitate the explicit approach and give an addition law with the main goal of proving associativity.

The novel (viewpoint)/thing is the construction over -any- field (excluding certain characteristics).

References

[1] J.W.S. Cassels and E.V. Flynn, "Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2", *Cambridge University Press*, 1996

[2] A. Menezes, Y.-H. Wu, and R. Zuccherato, "An Elementary Introduction to Hyperelliptic Curves", in "Algebraic Aspects of Cryptography", *Springer-Verlag*, 1998.
(`http://math.uwaterloo.ca/~ajmeneze/publications/hyperelliptic.pdf`)

[3] David Masser, "Elliptische Kurven I", *University of Basel, unpublished.*

[4] David Grant, "On an Analogue of the Lutz-Nagell Theorem for Hyperelliptic Curves", *Journal of Number Theory, to appear.*
(`euclid.colorado.edu/~grant/publications/lutznagellresubmit.pdf`)