Bisection and trisection polynomials for genus 2.

For every divisor $D$ in the Jacobian of a genus 2 curve $C : y^2 = f(x)$ over a field $k$, we compute a polynomial $p_D(x) \in k[x]$ with the following property:

\[ \exists D' \in \text{Jac}(C)(k) \mid 2D' = D \iff \exists \alpha \in k \mid p_D(\alpha) = 0. \]

Let $D_2 = [u_2(x), v_2(x)] \in \text{Jac}(C)(k)$. The set $\frac{1}{2}D_2 = \{ D \in \text{Jac}(C)(k) \mid 2D = D_2 \}$ is parametrised by the slope $m_1$ of a line $m_D(x) = m_1 x + m_0$ hidden in Cantor’s doubling algorithm, where momentarily the unreduced 1st coordinate $u_2(x)$ looks like

\[ \frac{f(x) - (m_D(x)u_2(x) - v_2(x))^2}{-m_1^2 u_2(x)}. \]

Equating with

\[ u(x)^2 = (x^2 + u_1 x + u_0)^2 \]

one obtains 4 equations in 4 variables $m_1, m_0, u_1, u_0$ whose solution $p_D(x)$ depends on $D_2$ and the $f(x)$ only. Our $p_D(x)$ has been used in point counting and in the computation of periods of curves of genus 1 and 2. Exchanging 2 by 3, our method can be further pushed to compute the whole 3-torsion subgroup and trisections of divisors in Jacobians of genus 2 curves in even characteristic. This is joint work with Josep M. Miret, Ana Rio and Nicolas Thériault. (Received January 28, 2019)