Periods modulo p of integer sequences associated with division polynomials of genus 2 curves

arXiv: 2310.01013

Yasuhiro Ishitsuka (Kyushu University)

j.w. w/ T. Ito (Kyoto), T. Ohshita (Gunma), T. Taniguchi (Kobe), Y. Uchida (Tokyo Metropolitan University)

Jul. 16, 2024

$(c_n)_{n\geq 0}$: the integer sequence A058231 in OEIS:

$$0, 0, 1, 36, -16, 5041728, -19631351040, -62024429150208, \dots.$$

- The sequence is defined as $c_n = \psi_{n,C}(P)$, where $\psi_{n,C}$ $(n \geq 0)$ are Cantor's division polynomials of

$$C: Y^2 = X^5 - 3X^4 - 2X + 9, \quad \text{and} \quad P = (0, 3).$$

- It satisfies a Somos-8 type quadratic recurrence

$$\begin{aligned} c_n c_{n+8} = & -11343888 c_{n+1} c_{n+7} + 14701679104 c_{n+2} c_{n+6} \\ & + 1590139434240 c_{n+3} c_{n+5} + 19631351040 c_{n+4}^2. \end{aligned}$$

Theorem (an example of I.–Ito–Ohshita–Taniguchi–Uchida, 2023)

- For all but finite prime p, $(c_n \bmod p)_{n\geq 0}$ is periodic.
- Its period is estimated as $\leq (p-1)(1+\sqrt{p})^4$.

Sketch of Proof:

1. For any $n \geq 0$ and a general prime p, at least one of $c_n, c_{n+1}, c_{n+2}, c_{n+3}$ mod p is nonzero (Cantor 1994).
2. Derive four recurrences

$$c_n c_{n+8} = \dots, \quad c_n c_{n+9} = \dots, \quad c_n c_{n+10} = \dots, \quad c_n c_{n+11} = \dots$$

   (from Weierstrass' identities on hyperelliptic sigma functions, 1882).
3. Let r be the order of the divisor $D_p = P - \infty \in \mathrm{Jac}(C)(\mathbb{F}_p)$. Then we inductively prove that, for constants $\alpha_p, \beta_p \in \mathbb{F}_p^\times$ and $a \geq 0$,

$$c_{ar+n} \equiv \alpha_p^a \beta_p^{a^2} c_n \mod p$$

   with the four recurrences. Substitute $a = p - 1$.
4. The last estimate follows from Hasse–Weil bound $|\mathrm{Jac}(C)(\mathbb{F}_p)| \leq (1 + \sqrt{p})^4$. $\square$