Modular Polynomial Symmetries

Semjon Adlaj (CCRAS, Moscow, Russia)

Calculating the roots of the modular equation of level p is tightly intertwined with calculating the p-torsin points on a corresponding elliptic curve. Galois must (surprisingly) be solely and entirely credited for pointing out this wonderful interplay. While Galois' contribution to formulating necessary and sufficient condition for solving algebraic equations via radicals is widely known, his decisive contribution to actually solving the quintic is barely (if at all) recognized. He is often credited for introducing the concept of irreducibility of an algebraic equation, but rarely (if ever) for introducing the concept of depressing the degree of an algebraic equation. Marvellously, he went on to indicate necessary and sufficient condition for depressing the degree of the modular equation of prime level, and, in particular, did display that the (Galois) group of modular equation of level 5 coincides with the group of the (general) quintic. He did write down an explicit construction for depressing the degree of the modular equation, of level 5, from 6 to 5. These contributions were apparently concealed by Hermite, under (much) influence from Cauchy, who (likely) privately shared with him some of Galois' "lost" papers, and, subsequently, concealed by Klein (who much praised Cauchy) to leave many researches (who did not read Galois' last letter) in oblivion as to the source of Hermite and Klein ideas, still (mistakenly) attributing to Hermite (and to Klein) finding the key for, eventually, solving the quintic. We shall, once and for all, lift the instillation that Galois' contribution to the theory of algebraic equation was limited to what has classically become known as Galois theory (however deep and however constructive, contrary to misguided perceptions), and we shall follow Galois' lead to arrive at a new class of bewildering (modular) polynomial identities, made readily accessible when tackled via the ingenious conceptual tools he left to us, but impenetrable to straightforward verifications, even if aided by contemporary computing machines, equipped with an up-to-date symbolic software packages. Even the simplest case of such identities, corresponding to the first odd prime 3, which was forwarded to several researchers on computer algebra, has withstood and will, most likely, withstand all machine pressure at cracking it, before this PCA 2014 conference. It (let alone the general case) might already motivate further required development of symbolic simplification (of algebraic formulas) procedures, being exposed as unsatisfactory. The case, corresponding to the second odd prime 5, might, also, be worthwhile to single out, here, as it would enable a (vivid) geometric interpretation of Galois' insightful construction, which was by no means exhausted by his many inspired followers (let alone Hermite and Klein), including those who were gracious to admit his exceptional, never nearly surpassable and far from fully appreciated, impact.