AGM and Jellyfish Swarms of Elliptic Curves

Michael J. Griffin, Ken Ono, Neelam Saikia, and Wei-Lun Tsai

Abstract. The classical AGM produces wonderful infinite sequences of arithmetic and geometric means with common limit. For finite fields $\mathbb{F}_q$, with $q \equiv 3 \pmod 4$, we introduce a finite field analogue $\mathrm{AGM}_{\mathbb{F}_q}$ that spawns directed finite graphs instead of infinite sequences. The compilation of these graphs reminds one of a *jellyfish swarm*, as the 3D renderings of the connected components resemble *jellyfish* (i.e., tentacles connected to a bell head). These swarms turn out to be more than the stuff of child's play; they are taxonomical devices in number theory. Each jellyfish is an isogeny graph of elliptic curves with isomorphic groups of $\mathbb{F}_q$-points, which can be used to prove that each swarm has at least $(1/2 - \varepsilon)\sqrt{q}$ jellyfish. This interpretation also gives a description of the *class numbers* of Gauss, Hurwitz, and Kronecker which is akin to counting types of spots on jellyfish.

1. ARITHMETIC AND GEOMETRIC MEANS. Beginning with positive real numbers $a_1 := a$ and $b_1 := b$, the $\mathrm{AGM}_{\mathbb{R}}$ inductively produces a sequence of pairs $\mathrm{AGM}_{\mathbb{R}}(a,b) := \{(a_1,b_1),(a_2,b_2),\ldots\}$, consisting of arithmetic and geometric means. Namely, for $n \geq 2$, we let

$$a_n := \frac{a_{n-1}+b_{n-1}}{2} \quad \text{and} \quad b_n := \sqrt{a_{n-1}b_{n-1}}.$$

For $n \geq 2$, we have the elementary inequality $a_n \geq b_n$. At a deeper level, the classical theory of the $\mathrm{AGM}_{\mathbb{R}}$ (for example, see Chapter 1 of [3]) establishes that these rapidly converging sequences have a common limit $\lim_{n\to+\infty} a_n = \lim_{n\to+\infty} b_n$.

In 1748, Euler [3] employed $\mathrm{AGM}_{\mathbb{R}}(\sqrt{2}, 1)$ as a remarkable device for rapidly computing digits of π. Namely, he showed that $\pi = \lim_{n\to+\infty} p_n$, where