

Linear Divisibility Recurrence Sequences and Primality Testing

The 2-term linear recurrence sequences had been studied by Lucas, Lehmer, etc. . . . These sequences have been used in primality testing. Rotkiewicz constructed infinitely many pseudoprimes (composites that behave like primes with respect to this test) in any arithmetic progression $ax + b$ with a and b relatively prime integers.

Let $f(x)$ be an irreducible polynomial of degree s with zeros $\alpha_1, \alpha_2, \dots, \alpha_s$ in the extension $K = \mathbf{Q}(\alpha_1, \alpha_2, \dots, \alpha_s)$ of \mathbf{Q} . Let \mathcal{G} be the Galois group of K over \mathbf{Q} . Then \mathcal{G} acts on the set of unordered pairs of roots of $f(x) = 0$ by $\sigma(\{\alpha_i, \alpha_j\}) = \{\sigma(\alpha_i), \sigma(\alpha_j)\}$ for each element σ of \mathcal{G} . Let \mathcal{O} be the orbit of the pair $\{\alpha_i, \alpha_j\}$ under this action. In my thesis, I study the divisibility sequences

$$D_0(n) = \prod (\alpha_i^n - \alpha_j^n) / (\alpha_i - \alpha_j)$$

where the product is over the unordered pairs $\{\alpha_i, \alpha_j\}$ in the orbit \mathcal{O} . I call them discriminant sequences.

A primality test analogous to the one using two-term linear recurrence sequences is devised for these sequences also. Composites that behave like primes are again called pseudoprimes. Infinitely many pseudoprimes of the form $ax + b$, with a and b relatively prime, are constructed in the manner of Rotkiewicz.

As examples, I consider the sequences coming from irreducible quartics and cubics, and study in a more detailed manner these discriminant sequences.

Finally, in the cubic case, a comparison is made between the primality test results using my discriminant sequences and those using the Adams-Shanks sequences defined by $A(n) = \alpha^n + \beta^n + \gamma^n$ where α, β, γ are the zeros of the irreducible cubic.