The Diverse Faces of Arithmetic: Postgraduate Lecture (Tom Ward)

December 14 2009

Recurrence Sequences

Definition 1.1. A sequence $a = (a_n)$, $n \in \mathbb{N}$ or $\mathbb{Z}$ (and typically with $a_n \in \mathbb{Z}$) is a *recurrence sequence* if there is some function Φ such that

$$a_{n+k} = \Phi(a_{n+k-1}, a_{n+k-2}, \ldots, a_n) \ \forall n$$

with initial conditions $a_0, \ldots, a_{k-1}$ determined.

One should pay attention to whether the index set starts at $n = 0$ or 1, and whether the sequence can be extended backwards.

- a is a *divisibility sequence* if $m|n \Rightarrow a_m|a_n \ \forall m, n$ (example: The Mersenne numbers $2^n - 1$)
- a is a *strong* divisibility sequence if

$$gcd(a_m, a_n) = a_{gcd(m,n)} \ \forall m, n$$

- $q \mid a_n$ is a *primitive divisor* if $q \nmid a_m$ for $m < n$.

Theorem 1.2. *Zsigmondy ($\beta = 1$), Bang (any β), others*
If

$$a = (\alpha^n - \beta^n) \ \alpha, \beta \in \mathbb{Z} \text{ coprime}$$

then

$$n \geq 6 \Rightarrow a_n \text{ has a primitive divisor.}$$

So, setting

$$Z(a) = \max\{n \,|\, a_n \text{ does not have a primitive divisor}\}$$

we have

$$Z((\alpha^n - \beta^n)) \leq 6$$

Meta-questions

- Given a class of recurrence sequences, can you bound Z across them?
  - Effectively?
  - Uniquely?
  - Small-ly?
- How big is the primitive part?

Linear Case

Here we are interested in sequences such that Φ is linear.

Example 1.3. The Fibonacci numbers $1, 1, 2, 3, 5, 8, \ldots$

This falls into the set of sequences with general term of form $A\rho^n + B(1/\rho)^n$.

Example 1.4. The Lucas numbers $1, 3, 4, 7, 11, \ldots$

This falls into the *trace class* of sequences with general term of form $\rho^n \pm (1/\rho)^n$ (i.e., special case of the above with $A = B = 1$); the terms arise as the trace of matrix powers, so there are many more techniques available for their analysis.

If a is an integral sequence with quadratic characteristic polynomial, then a is described as a Lucas/Lehmer sequence.

Theorem 1.5. *If a is Lucas/Lehmer, then $Z(a) \leq 30$ (and this bound is sharp).*

This was the first big, interesting theorem in this area since Zsigmondy's (100 year old) result, using all the weapons of modern diophantine analysis.

Bilinear Case

Remark 1.6. *There are many equivalent but subtly different ways to "see" these!*

Let E be an Elliptic curve over $\mathbb{Q}$ in generalised Weierstrass form. By the Mordell-Weil Theorem, $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$ for T some finite group and r the *rank* of E.

Definition 1.7. Given $P = (x(P), y(P))$ a non-torsion point of $E(\mathbb{Q})$, there exist A_n, B_n such that $x([n]P) = A_n/B_n$ (in lowest terms). Then $B = (B_n)$ is an *elliptic divisibility sequence* (EDS).

Such a B grows *really* fast- the number of decimal digits grows quadratically! (*quadratic exponential growth*).

Recall

$$Z(a) = \max\{n \mid a_n \text{ does not have a primitive divisor}\}$$

Silverman has shown that $Z(B)$ is always finite - i.e., for any EDS, there exists N such that (n$\geq$ N) $\Rightarrow$ (a_n has a primitive divisor). Given a "reasonable" family of curves, there are good (e.g., 3,7,13) explicit bounds for $Z(B)$. (work by Everest,Mclaren,Ward; Ingram,...)

Integrability/Laurent Phenomena

Remark 1.8. *It's often obvious why a recurrence sequence is integral, but there are some surprises.*

Definition 1.9. Consider a sequence subject to the constraint

$$u_{m+n}u_{m-n} = u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2 \text{ for all} m, n$$

with initial conditions satisfying

$$u_0 = 0, u_1 = 1, u_2u_3 \neq 0, u_2 \mid u_4$$

Then $u = (u_n)$ is a *somos sequence*.

Example 1.10. "Somos-4"

$$1, 1, 1, 1, 2, 3, 7, 23, 59, 314, 1529, \ldots$$

A Somos sequence is an integral divisibility sequence. One proof: they're EDS. But it can also be shown that each u_n is the solution to a counting problem on graphs, which is necessarily an integer.

Laurent Phenomena

For fixed $\alpha, \beta \in \mathbb{Q}$, consider a sequence satisfying

$$u_{n+4}u_n = \alpha u_{n+3}u_{n+1} + \beta u_{n+2}^2$$

As u_n is a rational function of α, β and the u_i, we trivially have that

$$u_n \in \mathbb{Z}(\alpha, \beta, u_1^{\pm 1}, u_2^{\pm 1}, u_3^{\pm 1}, u_4^{\pm 1})$$

However, we have (Fomin-Zelevinsky) the surprising stronger result that

$$u_n \in \mathbb{Z}[\alpha, \beta, u_1^{\pm 1}, u_2^{\pm 1}, u_3^{\pm 1}, u_4^{\pm 1}]$$

i.e., u_n is a Laurent polynomial in the intial conditions and α, β.

Growth

Lehmer-Pierce Sequences

Let $f \in \mathbb{Z}[x]$ factor over $\mathbb{C}$ as $f(x) = (x - \alpha_1) \cdots (x - \alpha_d)$. For each n, let

$$\Delta_n(f) = \prod_{i=1}^{d} |\alpha_i^n - 1|$$

Then $\Delta_n(f) \in \mathbb{Z}$ (an 'old fashioned proof' is possible via symmetric polynomials; a more modern approach would be via Galois theory).

Assume $\Delta_n(f) \neq 0$ for all $n \geq 1$. How big is $\Delta_n(f)$?

Note:

- $|\alpha_i| < 1 \Rightarrow |\alpha_i^n - 1| \to 1$.
- $|\alpha_i| > 1 \Rightarrow |\alpha_i^n - 1|^{\frac{1}{n}} \to |\alpha_i|$.
- $|\alpha_i| = 1 \Rightarrow ?$ (Such α_i still exist- the assumption only excludes *unit* roots)
  - There exists (n_j) such that $|\alpha_i^{n_j} - 1| \to 0$.

Definition 1.11. For $\log^+ x = \max\{\log x, 0\}$, the *logarithmic Mahler measure* of f is

$$M_f := \sum_{i=1}^{d} \log^+ |\alpha_i| = \int_0^1 \log |f(e^{2\pi i t})| dt$$

Then there exists $A = A(f) > 0$ such that

$$\frac{1}{n} \log \Delta_n(f) = M_f + O\left(\frac{(\log n)^A}{n}\right)$$

Lehmer's Problem

Kronecker's Lemma: $M_f = 0 \Rightarrow f$ is a product of cyclotomics.

Does there exist a $c > 0$ such that $M_f > 0 \Rightarrow M_f > c$? It is conjectured that this is the case- the smallest known example is Lehmer's Polynomial, with $M_f = 0.162\ldots$.

Theorem 1.12. *If u is a nontrivial EDS, then there exist $K > 0, A > 0$ such that*

$$log\,|u_n| = Kn^2 + O((log\,n)^A)$$

Meta-conjectures

(There may be trivial counterexamples, but if not, these are expected to be true.)

u a nontrivial EDS $\Rightarrow$

- u_n prime finitely often (except for the understood cases where not);
- u_n a product of $\leq K$ primes finitely often;
- primitive part of u_n huge.

u a linear recurrence sequence $\Rightarrow$ u_n a product of $\leq K$ primes infinitely often.