Maximal Divisors

Of Certain Quartic Linear Recurrences

Amy Goldlist

University of British Columbia

March 15, 2007

Outline

1. Linear Recurrences
2. Division Properties
3. Plan of Attack
4. The Main Sequence
5. Conclusion

Linear Recurrences

A Linear Recurrence Sequence (of degree m) is a sequence $V = \{v_n\}$, determined by:

- m initial values: $v_0, v_1, ..., v_{m-1}$; and
- A rule for finding all other values:

$$v_n = P_1 v_{n-1} + P_2 v_{n-2} + ... + P_m v_{n-m}$$

The rule determines a Polynomial

$$f(x) = x^m - P_1 x^{m-1} - \cdots - P_m$$

If g is a polynomial for a sequence V, and $g|f$, then f is also a polynomial for V. We call the minimum such polynomial the Characteristic Polynomial of V.

Other Ways of Writing a Sequence

If $V = \{v_n\}$ is a sequence with polynomial $f(x) = \prod_i (x - \theta_i)$, then it is possible to write our sequence as:

$$v_n = \sum_{i=1}^{m} \alpha_i \theta_i^n$$

for an appropriate choice of α_i.
We can also rewrite our sequence as:

$$v_n = \frac{1}{\delta} \sum_{k=1}^{m} \Delta_i A_i \theta_i^n$$

where $\delta = \prod_{i<j} (\theta_j - \theta_i) = \begin{vmatrix} 1 & \cdots & 1 \\ \theta_1 & \cdots & \theta_m \\ \vdots & \ddots & \vdots \\ \theta_i^{m-1} & \cdots & \theta_m^{m-1} \end{vmatrix}$ is the discriminant of f.

Other Ways of Writing a Sequence

And

$$\Delta_i = \begin{vmatrix} 1 & \cdots & 0 & \cdots & 1 \\ \theta_1 & \cdots & 0 & \cdots & \theta_m \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \theta_1^i & \cdots & 1 & \cdots & \theta_m^i \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \theta_1^{m-1} & \cdots & 0 & \cdots & \theta_m^{m-1} \end{vmatrix}$$

where the ith column has been switched to zeros with a 1 in the ith row.

Note that $\Delta_i = \dfrac{\pm\delta}{\prod_{j\neq i}(\theta_i - \theta_j)}$.

So, $A_i = \dfrac{\alpha_i \delta}{\Delta_i}$.

Other Ways of Writing a Sequence

This is called Standard Form, and we write our sequence V as

$$v_n = \frac{1}{\delta} \sum_{k=1}^{m} \Delta_i A_i \theta_i^n$$

or $V =< A_1, A_2, ..., A_m >$.
Every sequence obeying $f(x)$ can be uniquely determined by the A_i.

Definition

The set of recurrences obeying $f(x)$ is $\mathcal{L}(f)$. We say that two sequences $< A_1, \ldots A_m >$ and $< B_1, \ldots B_m >$ are equivalent if $< A_1, \ldots A_m >= \lambda < B_1, \ldots B_m >$ for some $\lambda \neq 0$. With this equivalence, we have a group under the operation $*$, where:

$$< A_1, \ldots A_m > * < B_1, \ldots B_m >=< A_1 B_1, \ldots A_m B_m > .$$

This is called the Laxton-Ballot Group of f, $L - B(f)$.

Outline

1. Linear Recurrences
2. Division Properties
3. Plan of Attack
4. The Main Sequence
5. Conclusion

Division Properties of a Sequence

- A prime p divides V if it divides v_n for some n.
- p trivially divides V (at n) if there exists N such that $p|v_n$ for all $n > N$.
- p maximally divides V if $p|v_{n+i}$ for $i = 0, 1, \cdots m - 2$, and $p \nmid v_{n+m-1}$. That is, p divides $m - 1$ consecutive terms, but is not a trivial divisor.

One of the important properties of the Laxton-Ballot group is that it preserves division properties.

Some Questions

- Given a sequence V, what is the (relative) density of primes which divide V?
- Given a sequence V, what is the (relative) density of primes which maximally divide V?
- Given a polynomial $f(x)$, is there a sequence V which obeys it, such that we can calculate the (relative) density of primes which divide it?

Algebra We Will Need

We begin with some terminology:

- Given our polynomial $f(x)$, let $K = \mathbb{Q}(\theta_1, \theta_2, \cdots \theta_m)$ be the splitting field of f.
- Let $\mathcal{O}_K$ be the Ring of Integers of K.
- Let ζ_{2^j} be a primitive 2^jth root of unity, and $\mathbb{Q}(\zeta_{2^j})$ be the 2^jth cyclotomic field.

We will also need:

Theorem

The Chebotarev Density Theorem *(Easy Version). The density of primes which split completely from K to L is $1/[L : K]$.*

An Important Lemma

Lemma

***(Ballot)** A prime p, where $p \nmid 2\delta P_i$ maximally divides the sequence*

$$V =< A_1, \dots A_m >= \left\{ v_n = \frac{1}{\delta} \sum_{k=1}^{m} \Delta_i A_i \theta_i^n \right\}$$

at n with polynomial $f(x)$ if and only if:

$$A_1\theta_1^n \equiv A_2\theta_2^n \equiv \cdots \equiv A_m\theta_m^n \mod (p)$$

Where $(p) \subset \mathcal{O}_K$ is the ideal generated by p in $\mathcal{O}_K$.

Proof.

Straightforward computation using properties of Vandermonde Determinants. □

Outline

1. Linear Recurrences
2. Division Properties
3. Plan of Attack
4. The Main Sequence
5. Conclusion

Plan of Attack

1. Pick a family of polynomials, f
2. Pick a sequence $V =< A_1, A_2, \cdots A_m >$ which is integral, and which has the property that $A_i/A_j = \pm 1$. This is equivalent to saying that V has order 2 in $L - B(f)$.
3. Partition the primes in a clever fashion.
4. Use the Lemma to rephrase the question of p maximally dividing V into a question about the order of θ_i/θ_j mod(p).
5. Turn this into a condition about how p splits in a series of field extensions.
6. Use the Chebotarev Density Theorem to translate this back into a density.

What Has Been Done So Far

- $2^n + 1$, so $f(x) = x^2 - 3x + 2$. (Hasse)
- $a^n + b^n$, where $a, b \in \mathbb{Z}$. Here f is reducible and quadratic. (Lucas, Ballot)
- $\alpha^n + (-\alpha)^n$, α of degree 2 over $\mathbb{Q}$. Here f is quadratic and irreducible. (Lagarias)
- f is in a certain family of cubics. (Ballot, Luca)

Outline

1. Linear Recurrences
2. Division Properties
3. Plan of Attack
4. The Main Sequence
5. Conclusion

A Choice For f

Choose D_1 and $D_2 \in \mathbb{Z}$ such that

- They are not perfect squares.
- The absolute values of their square-free parts are distinct, That is, if $d_1 = \sqrt{D_1}$ and $d_2 = \sqrt{D_2}$ then $\mathbb{Q}(d_1) \neq \mathbb{Q}(d_2)$ and $\mathbb{Q}(d_1/d_2) \neq \mathbb{Q}(i)$.
- Let E_1 and E_2 be the square free parts of D_1 and D_2, respectively.

Let:

$$\begin{aligned}
\theta_1 &= 1 + d_1 + d_2 + d_1 d_2 \\
\theta_2 &= 1 - d_1 + d_2 - d_1 d_2 \\
\theta_3 &= 1 + d_1 - d_2 - d_1 d_2 \\
\theta_4 &= 1 - d_1 - d_2 + d_1 d_2
\end{aligned}$$

A Choice For f

Then we set:

$$f(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4)$$

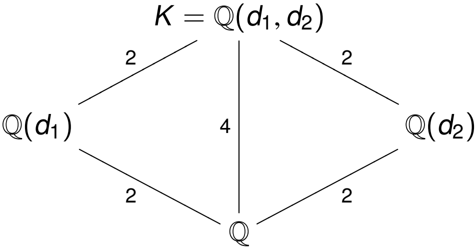
Expanding we get:

- $f(x) = x^4 - 4x^3 + (6 - 2d_1^2 - 2d_2^2 - 2d_1^2 d_2^2)x^2 + (4d_1^2 + 4d_2^2 - 4d_1^2 d_2^2 - 4)x + (1 - 2d_1^2 - 2d_2^2 + 4d_1^2 d_2^2 - 2d_2^4 d_1^2 + d_1^4 + d_2^4 - 2d_1^4 d_2^2 + d_1^4 d_2^4)$
- And $f(x) = x^4 - 4x^3 + (6 - 2D_1 - 2D_2 - 2D_1 D_2)x^2 + (4D_1 + 4D_2 - 4D_1 D_2 - 4)x + (1 - 2D_1 - 2D_2 + 4D_1 D_2 - 2D_1 D_2^2 + D_1^2 + D_2^2 - 2D_1^2 D_2 + D_1^2 D_2^2)$

A Choice For f

By our choice of f, $f(x)$ is irreducible over $\mathbb{Z}$, and its splitting field is $K = \mathbb{Q}(d_1, d_2)$, with Galois Group $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the Klein-4 group.

We have the following field extension:



A Choice For *f*

Then we have:

$$\begin{aligned}\delta &= \prod_{1\le j<k\le 4} (\theta_k - \theta_j) \in \mathbb{Z}\\ &= 2^6 D_1 D_2 (D_1 - 1)(D_2 - 1)(D_2 - D_1) \in \mathbb{Z}\\ &\text{and}\\ \Delta_1 &= -(\theta_4 - \theta_3)(\theta_4 - \theta_2)(\theta_3 - \theta_2)\\ &= 2^3 d_1 d_2 (d_2 - d_1)(d_1 - 1)(d_2 - 1)\\ \Delta_2 &= (\theta_4 - \theta_3)(\theta_4 - \theta_1)(\theta_3 - \theta_1)\\ &= 2^3 d_1 d_2 (d_2 - 1)(d_1 + d_2)(d_1 + 1)\\ \Delta_3 &= -(\theta_4 - \theta_2)(\theta_4 - \theta_1)(\theta_2 - \theta_1)\\ &= 2^3 d_1 d_2 (1 - d_1)(d_1 + d_2)(1 + d_2)\\ \Delta_4 &= (\theta_3 - \theta_2)(\theta_3 - \theta_1)(\theta_2 - \theta_1)\\ &= 2^3 d_1 d_2 (d_1 - d_2)(1 + d_1)(1 + d_2)\end{aligned}$$

Choosing V

Given f, we choose:

$$V = \{v_n\} =< -\delta d_1 d_2, \delta d_1 d_2, \delta d_1 d_2, -\delta d_1 d_2 >$$

Lemma

V is a sequence of rational integers.

Proof.

Since we know that all of the entries are integers in O_K, by noting that the denominator was canceled out by multiplying through by δ we can look at the automorphisms of K. We look at the Gal$(K/\mathbb{Q})$. Remember, it is isomorphic to the Klein-4 group, so it is generated by 2 automorphisms of order 2. Let $\sigma : d_1 \mapsto -d_2$ and $\tau : d_2 \mapsto -d_2$. Then, using permutation notation:

$$\sigma = (\theta_1, \theta_2)(\theta_3, \theta_4)$$

and

$$\tau = (\theta_1, \theta_3)(\theta_2, \theta_4)$$

or

$$\sigma = (\Delta_1, \Delta_2)(\Delta_3, \Delta_4)$$

and

$$\tau = (\Delta_1, \Delta_3)(\Delta_2, \Delta_4).$$

It is now clear that both sequences are rational, we just apply σ and τ and observe that they remain constant. □

Partitioning Primes in a Clever Way

- First, we eliminate all of the bad primes which Ballot's Lemma did not work for, that is all p such that $p \mid 2\delta P_i$.
- These are exactly the primes which trivially divide V, and correspond to the primes which are ramified from $\mathbb{Q}$ to K.
- Since there are only finitely many of these, it will not affect our count.
- In order to continue, we will need to find the order of the group mod (p), that is, $|\mathcal{O}_K/(p)|$.

Partitioning Primes in a Clever Way

We have three case to look at:

1. p is totally inert in K (has an inertial degree, $\mathfrak{f} = 4$), that is $(\frac{E_1}{p}) = (\frac{E_2}{p}) = -1$, where $(\frac{\cdot}{p})$ is the Legendre symbol. In this case, algebraic number theory tells us that:

$$|\mathcal{O}_K/(p)| = 4|\mathbb{Z}/p\mathbb{Z}| = 4(p-1)$$

2. p is inert in only one of the quadratic subfields of K, that is, $(\frac{E_1}{p}) \cdot (\frac{E_2}{p}) = -1$. Again, we find that our inertial degree is $\mathfrak{f} = 2$, and so:

$$|\mathcal{O}_K/(p)| = 2|\mathbb{Z}/p\mathbb{Z}| = 2(p-1)$$

3. p is totally split in K, that is the inertial degree is $\mathfrak{f} = 1$ and $(\frac{E_1}{p}) = (\frac{E_2}{p}) = 1$. Then

$$|\mathcal{O}_K/(p)| = |\mathbb{Z}/p\mathbb{Z}| = p - 1$$

Partitioning Primes in a Clever Way

First, we recall that $v_2(a) = j$ means that $2^j | a$ but $2^{j+1} \nmid a$.
Let

$$S^j := \{p : v_2(p-1) = j\},$$

And we further partition:

$$S^j_i := \{p \in S^j : v_2(\mathfrak{f}) = i\}$$

where $\mathfrak{f}$ is the inertial degree of (p) in $\mathcal{O}_K$.
Now we see that:

$$|\mathcal{O}_K/(p)| = 2^i(p-1) = 2^{i+j}B$$

where B is odd.

Getting to Orders

We need some extra notation:

$$\psi_1 = \frac{\theta_1}{\theta_2}, \psi_2 = \frac{\theta_1}{\theta_3}, \psi_3 = \frac{\theta_2}{\theta_4}, \psi_4 = \frac{\theta_3}{\theta_4}, \psi_5 = \frac{\theta_1}{\theta_4}, \psi_6 = \frac{\theta_2}{\theta_3},$$

Recall p is a maximal divisor of V if :

$$\theta_1^n = -\theta_2^n = -\theta_3^n = \theta_4^n \mod (p),$$

that is Ballot's Lemma tells us that in order for a specific p to divide V maximally, we need the following conditions to hold:

$$\begin{aligned}
\psi_1^n &\equiv -1 \mod (p)\\
\psi_2^n &\equiv -1 \mod (p)\\
\psi_3^n &\equiv -1 \mod (p)\\
\psi_4^n &\equiv -1 \mod (p)\\
\psi_5^n &\equiv 1 \mod (p)\\
\psi_6^n &\equiv 1 \mod (p)
\end{aligned}$$

Getting to Orders

Making life easier for us:

- $\psi_1 = \psi_4$ via "simple" computation.
- $\psi_3 = \psi_2$.
- By definition, $\psi_5 = \psi_1/\psi_3$, thus if $\psi_1^n \equiv -1$ and $\psi_3^n \equiv -1$, then $\psi_5^n = (\psi_1/\psi_3)^n \equiv -1/-1 \equiv 1$.
- Similarly $\psi_6^n \equiv 1$ if $\psi_2^n \equiv -1$.

Letting $v_2(\mathrm{ord}_{(p)}(\psi)) = v(\psi)$, we see the real conditions is:

Theorem

p divides V maximally if and only if $v(\psi_1) = v(\psi_2) > 0$.

Splitting Conditions (If Life Were Easy)

If there were only one ψ to worry about, we could say that if p is not a maximal divisor, then $v(\psi) = 0$:
Then for any n:

$$\psi^n \not\equiv -1 \mod (p)$$

So

$$\psi^{2^i(p-1)/2^{j+i}} \equiv 1 \mod (p)$$

And thus

$$X^{2^{j+i}} - 1$$

splits completely mod (p).
So, we Algebraic Number Theory tells us that if $\mathfrak{p}|(p) \subset \mathcal{O}_K$ is prime, $\mathfrak{p}$ splits completely from K to $K(\sqrt[2^{j+i}]{\psi})$.

Splitting Conditions (If Life Were Easy)

- $p \in S^j$ if and only if p splits completely from $\mathbb{Q}$ to $\mathbb{Q}(\zeta_{2^j})$ but not from $\mathbb{Q}$ to $\mathbb{Q}(\zeta_{2^{j+1}})$.
- This means that $v(\psi) = 0$, and $p \in S_i^j$ if and only if $\mathfrak{p}$ splits from K to $K(\sqrt[2^{j+i}]{\psi}, \zeta_{2^j})$, but not to $K(\sqrt[2^{j+i}]{\psi}, \zeta_{2^{j+1}})$.

This leads us to the following tower of field extensions:

$$\begin{tikzcd}
 & & M = L(\zeta_{2^{j+1}}) \arrow[dll, no head] \arrow[d, no head] \arrow[drr, no head] & & \\
M_1 = K_1(\zeta_{2^{j+1}}) \arrow[d, no head] & & L = K(\zeta_{2^j}, \sqrt[2^{j+i}]{\psi_1}, \sqrt[2^{j+i}]{\psi_2}) \arrow[dll, no head] \arrow[drr, no head] & & M_2 = K_2(\zeta_{2^{j+1}}) \arrow[d, no head] \\
K_1 = K(\zeta_{2^j}, \sqrt[2^{j+i}]{\psi_1}) \arrow[drr, no head] & & & & K_2 = K(\zeta_{2^j}, \sqrt[2^{j+i}]{\psi_2}) \arrow[dll, no head] \\
 & & K(\zeta_{2^j}) \arrow[dll, no head] \arrow[drr, no head] & & \\
K \arrow[drr, no head, "4"] & & & & \mathbb{Q}(\zeta_{2^j}) \arrow[dll, no head, "2^{j-1}"] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

Splitting Conditions (With An Added Complication)

Unfortunately, we have two ψ, and so just being odd is not enough. Instead we look at another tower of extensions:

- Let $l = 1, 2, ...j + i$.
- If $v(\psi) \leq l$, then:

$$\psi^{B2^l} \equiv 1 \mod (p)$$
$$\psi^{2^i(p-1)2^l/2^{j+i}} \equiv 1 \mod (p)$$
$$\psi^{2^i(p-1)/2^{j+i-l}} \equiv 1 \mod (p)$$

- and so:

$$X^{2^{j+i-l}} - 1$$

  splits completely mod (p).
- Following our earlier chain of logic, we have $v(\psi) \leq l$, and $p \in S_i^j$ if and only if $\mathfrak{p}$ splits completely from K to $K(\sqrt[2^{j+i-l}]{\psi}, \zeta_{2^j})$, but not to $K(\sqrt[2^{j+i-l}]{\psi}, \zeta_{2^{j+1}})$.

Splitting Conditions (With An Added Complication)

We need $v(\psi) = l$, not $\leq l$. So:

- For $1 \leq l \leq j + i$ $v(\psi) = l$ exactly iff: $\mathfrak{p}$ splits from K to $K(\sqrt[2^{j+i-l}]{\psi}, \zeta_{2^j})$, but not to $K(\sqrt[2^{j+i-l}]{\psi}, \zeta_{2^{j+1}})$, and not to $K(\sqrt[2^{j+i-l+1}]{\psi}, \zeta_{2^j})$.
- And I need this to happen simultaneously for both ψ_1 and ψ_2.

Splitting Conditions (With An Added Complication)

Diagrammatically we have:

$$\begin{tikzcd}
K_{1,l}(\zeta_{2^{j+1}}) & K_{1,l-1} & & K_{2,l-1} & K_{1,l}(\zeta_{2^{j+1}}) \\
& K_{1,l} \arrow[ul, dash] \arrow[u, dash] & & K_{2,l} \arrow[u, dash] \arrow[ur, dash] & \\
& & K(\zeta_{2^j}) \arrow[ul, dash] \arrow[ur, dash] & & \\
& & K \arrow[u, dash] & &
\end{tikzcd}$$

Translating Back to Densities

The density of primes which divide V should be:

- $\sum_{j=1}^{\infty} \sum_{l=1}^{j} \#$(primes which split completely from $\mathbb{Q}$ to K, $\mathbb{Q}(\zeta_{2^j})$, $K_{1,l}$ and $K_{2,l}$, but not to any of $\mathbb{Q}(\zeta_{2^{j+1}})$, $K_{1,l-1}$ or $K_{2,l-1}$)
- $+ \sum_{j=1}^{\infty} \sum_{l=1}^{j+1} \#$(primes which have inertial degree 2 from $\mathbb{Q}$ to K, and $\mathfrak{p}$ splits completely from K to $\mathbb{Q}(\zeta_{2^j})$, $K_{1,l}$ and $K_{2,l}$, but not to any of $\mathbb{Q}(\zeta_{2^{j+1}})$, $K_{1,l-1}$ or $K_{2,l-1}$)
- $+ \sum_{j=1}^{\infty} \sum_{l=1}^{j+2} \#$(primes which are inert from $\mathbb{Q}$ to K and p splits completely from K to $\mathbb{Q}(\zeta_{2^j})$, $K_{1,l}$ and $K_{2,l}$, but not to any of $\mathbb{Q}(\zeta_{2^{j+1}})$, $K_{1,l-1}$ or $K_{2,l-1}$)

By paying careful attention to details, this should be computable in most cases.

Translating Back to Densities

In many cases this will look something like:

- $\left(\frac{1}{[K:\mathbb{Q}]}\right)T_0+\left(\frac{1}{[\mathbb{Q}(d_1):\mathbb{Q}]}-\frac{1}{[K:\mathbb{Q}]}+\frac{1}{[\mathbb{Q}(d_2):\mathbb{Q}]}-\frac{1}{[K:\mathbb{Q}]}\right)T_1+$ $\left(1-\frac{1}{[K:\mathbb{Q}]}-\frac{1}{[\mathbb{Q}(d_1):\mathbb{Q})]}-\frac{1}{[\mathbb{Q}(d_2):\mathbb{Q}]}\right)T_2$
- Where $T_i=\sum_{j=1}^{\infty}\sum_{l=1}^{j+i}\frac{1}{[\mathbb{Q}(\zeta_{2^{j+1}}):\mathbb{Q}]}$ $\left(\frac{1}{[K_{1,l}:K(\zeta_{2^j})]}+\frac{1}{[K_{2,l}:K(\zeta_{2^j})]}-\frac{1}{[K_{1,l-1}:K(\zeta_{2^j})]}-\frac{1}{[K_{1,l-1}:K(\zeta_{2^j})]}\right)$
- And $K_{k,l}=K(\zeta_{2^j},\ \sqrt[2^{j+i-l}]{\psi_k})$.

Outline

1. Linear Recurrences

2. Division Properties

3. Plan of Attack

4. The Main Sequence

5. Conclusion

Conclusion

The theory of recurrence sequences is a subject deeply intertwined with such diverse mathematical topics as graph theory, Diophantine equations and dynamical sequences. Linear recurrence sequences form the mathematical basis for some of the most cutting edge modern cryptographic systems; with out growing reliance on computers, computer security is becoming an essential part of modern life. In fact, recurrence sequences are used to generate strings of uniformly distributed pseudo-random numbers. Such sequences can be shown to be predictable in polynomial time only, and thus are important in cryptography.

Selected References

Ballot, Christian, *Density of Prime Divisors of Linear Recurrences*, Memoirs of the American Mathematical Society, vol. 115, number 551, 1995.

Everest, Grahm; Alf van der Poorten; Igor Shparlinski and Thomas Ward, *Recurrence Sequences*, Providence: American Mathematical Society, 2003.

Laxton, R.R., *On Groups of Linear Recurrences. I.*, Duke Math Journal, 26, pp.721-736, 1969.