On polynomials attached to curves

F. Morain

Laboratoire d'Informatique de l'École polytechnique

logoUW

London, November 14th, 2008

Plan

I. Introduction.

II. Warming up: the genus 0 case.

III. The genus 1 case: elliptic curves.

IV. A glimpse at genus 2.

V. Conclusions.

I. Introduction and motivations

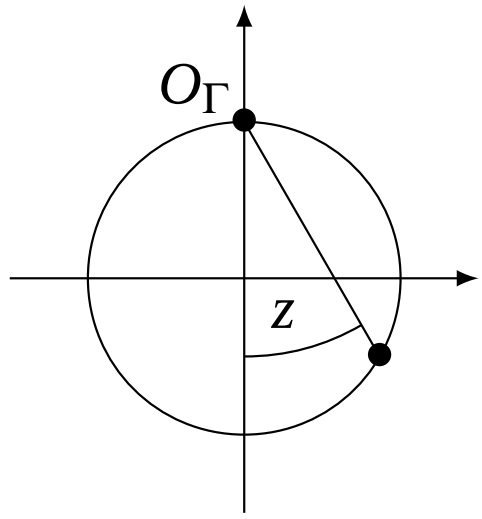
- Construct mathematical objects: cyclotomic fields, abelian extensions.
- Point counting on algebraic curves over finite fields. (Schoof-Elkies-Atkin algorithm, Pila, etc.).

In this talk: division polynomials, modular polynomials in genus ≤ 2.

II. Warming up: the genus 0 case

Circles

$\Gamma : y^2 = 1 - x^2$

$z \in (-\pi, \pi]$ 

We have a map:

$$\begin{array}{rccc} \wp : & \mathbb{C}/(2\pi\mathbb{Z}) & \to & \Gamma \\ & z & \mapsto & (\sin z, \cos z). \end{array}$$

Group law: inherited from $z_1 + z_2$ on the left and the neutral element is $\wp(0) = (0, 1)$. Formulas are polynomials.

Division polynomials

$$\wp([n](\sin z, \cos z)) = \wp(\sin(nz), \cos(nz))$$
$$= (\mathscr{S}_n(\sin z, \cos z), \mathscr{C}_n(\sin z, \cos z)).$$

Computing $\mathscr{S}_n$, $\mathscr{C}_n$: $O(\log n)$ polynomial operations using

$$\mathscr{S}_n(z) + i\mathscr{C}_n(z) = \exp(inz) = (\mathscr{S}_1(z) + i\mathscr{C}_1(z))^n.$$

An n-torsion point is $\sin(nz) = 0$, $\cos(nz) = 1$, that is $z = \exp(2ik\pi/n)$ for $k \in \{0, \ldots, n-1\}$. Equivalently, z is a root of $X^n - 1$.

$C_d(X) =$ minimal polynomial of z of order exactly d:

$$X^n - 1 = \prod_{d|n} C_d(X).$$

Some of the magical properties of $C_n(X)$

Fact: $C_d(X) \in \mathbb{Z}[X]$ is reciprocal.

$$C_\ell(X) = (X^\ell - 1)/(X-1) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1;$$

$$C_{\ell^e}(X) = C_\ell(X^{\ell^{e-1}}).$$

For $\gcd(n_1, n_2) = 1$:

$$C_{n_1 n_2}(X) = \frac{C_{n_1}(X^{n_2})}{C_{n_2}(X)}.$$

Möbius:

$$C_n(X) = \prod_{1 \le k \le n, k|n} (X^k - 1)^{\mu(k/n)}.$$

Algorithms:

- euclidean division (exact, but possible overflow);
- Brent (power sums + Newton, *Math. Comp.*);
- Monagan/Arnold (recent): Möbius + division of sparse series.

Height

$$C_n(X) = \sum_{k=0}^{\varphi(n)} a_n(k) x^k.$$

$$A(n) = \max_k |a_n(k)|, \quad \beta(n) = \sum_k |a_n(k)|$$

Thm. (Bateman, 1949) $\beta(n) \leq n^{d(n)/2}$.

Thm. (J.-L. Nicolas, G. Terjanian, 1999) for $n \geq 7$, $n \neq 10$,

$$\beta(n) < (\sqrt{2})^{\varphi(n)}.$$

Thm. (S. Konyagin, H. Maier, E. Wirsing, 2004) For fixed $C > 2/\log 2$ and $\mathscr{E}_C = \{n, \omega(n) \geq C \log\log n\}$, then for all $\varepsilon > 0$, there exists n_ε s.t. $n \geq n_\varepsilon$,

$$A(n) \geq \exp\left((\log n)^{C\log 2/2-\varepsilon}\right).$$

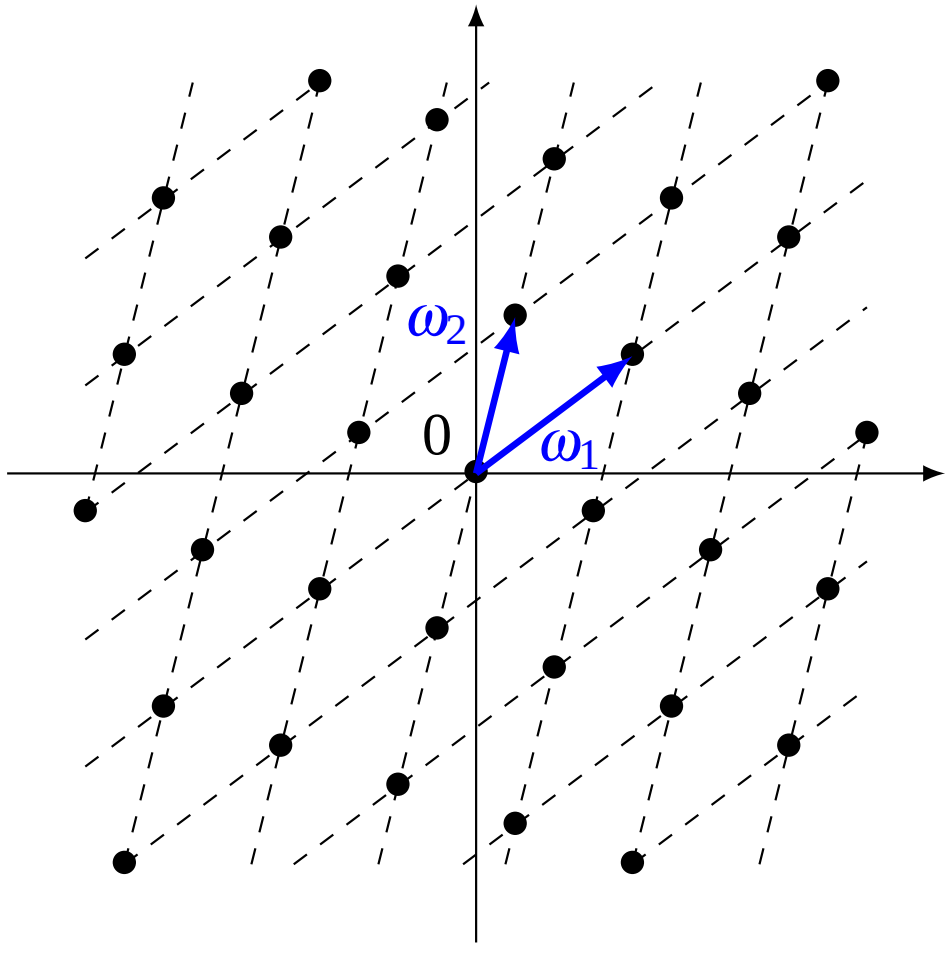
Monagan:

$$A(1880394945) = 64540997036010911566826446181523888971563.$$

III. The genus 1 case: elliptic curves

A) Lattices and the classical theory over $\mathbb{C}$

$$\mathscr{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \quad \tau = \omega_2/\omega_1 \in \mathscr{H}\{z \in \mathbb{C}, \Im(z) > 0\}$$



$\Rightarrow$ What are the periodic functions over $\mathscr{L}$?

Weierstrass's function

Def. f is an elliptic function iff

- f is doubly periodic: $f(z+\omega_i) = f(z)$;
- f is analytic (except at poles), with no finite singularities (except at poles)

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \mathscr{L},\, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Thm. $\wp$ is differentiable and:

$$\wp'(z) = -2 \sum_{\omega \in \mathscr{L}} \frac{1}{(z-\omega)^3}.$$

Prop. $\wp'$ and $\wp$ are periodic on $\mathscr{L}$.

Expansion of $\wp$ near the origin

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2(1-\frac{z}{\omega})^2} = \frac{1}{\omega^2} + \frac{2z}{\omega^3} + \cdots + \frac{kz^{k-1}}{\omega^{k+1}} + \cdots$$

Eisenstein series ($k \geq 2$):

$$G_k(\mathscr{L}) = \sum_{\omega \in \mathscr{L},\, \omega \neq 0} \frac{1}{\omega^k}$$

$$\wp(z) = \frac{1}{z^2} + 3z^2 G_4 + 5z^4 G_6 + \cdots$$

Rem. Fast expansion of $\wp$ in BoMoSaSc08.

Link with elliptic curves

$$g_2 = 60\,G_4, \quad g_3 = 140\,G_6$$

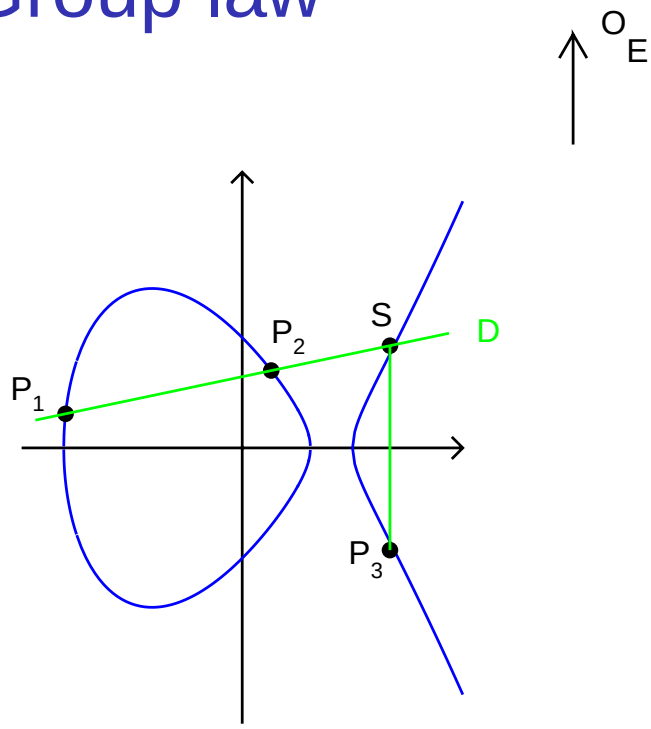
$$\forall\, z \in \mathbb{C} - \mathscr{L},\ \wp'^2(z) = 4\,\wp(z)^3 - g_2\,\wp(z) - g_3$$

We get a parametrization

$$\begin{array}{ccc} \mathbb{C} - \mathscr{L} & \to & E \\ z & \mapsto & (\wp(z), \wp'(z)) \end{array}$$

(and we send $\mathscr{L}$ to O_E.)

Group law



On $E : y^2 = x^3 + ax + b$, to find

$$(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2),$$

relate $\wp(z_1 + z_2)$ to $\wp(z_1)$ and $\wp(z_2)$.

$$P_1P_2 : y = \lambda x + \mu, \quad x_1 + x_2 + x_3 = -\lambda^2$$

with

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_2 \neq P_1 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } P_2 = P_1 \end{cases}$$

$\Rightarrow$ algebraic formulas; ditto for $[k]P = \underbrace{P \oplus \cdots \oplus P}_{k \text{ times}}$.

Division polynomials

for $E : y^2 = x^3 + Ax + B$

$$[n](X,Y) = \left(\frac{\phi_n(X,Y)}{\psi_n(X,Y)^2}, \frac{\omega_n(X,Y)}{\psi_n(X,Y)^3} \right)$$

$$\phi_n = X\psi_n^2 - \psi_{n+1}\psi_{n-1}, \quad 4Y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$$

$$\phi_n, \psi_{2n+1}, \psi_{2n}/(2Y), \omega_{2n+1}/Y, \omega_{2n} \in \mathbb{Z}[A,B,X]$$

$$f_n(X) = \begin{cases} \psi_n(X,Y) & \text{for } n \text{ odd} \\ \psi_n(X,Y)/(2Y) & \text{for } n \text{ even} \end{cases}$$

$$f_{-1} = -1, \quad f_0 = 0, \quad f_1 = 1, \quad f_2 = 1$$

$$f_3(X,Y) = 3X^4 + 6AX^2 + 12BX - A^2$$

$$f_4(X,Y) = X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3$$

Division polynomials (cont'd)

$$f_{2n} = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2)$$

$$f_{2n+1} = \begin{cases} f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}(16Y^4) & \text{if } n \text{ is odd} \\ (16Y^4)f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1} & \text{otherwise.} \end{cases}$$

$$\deg(f_n(X)) = \begin{cases} (n^2-1)/2 & \text{if } n \text{ is odd} \\ (n^2-4)/2 & \text{otherwise.} \end{cases}$$

Main use: Schoof-Elkies-Atkin algorithm.

Qi Cheng: direct use of these formulas require keeping only nine values of f_{n+k} at the same time.

McKee: exact formula for $[X^i]f_n$ (it is homogeneous in A and B with respective weights 4 and 6).

Dewaghe: polynoms of exact division (cyclotomic polynomials).

The invariant j

$$\Delta(\tau) = g_2^3(\tau) - 27\, g_3^2(\tau) = q \prod_{n \geq 1} (1 - q^n)^{24}$$

$$j(\tau) = 1728\, \frac{g_2^3(\tau)}{\Delta(\tau)}$$

$$j(q) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n\, q^n, c_n \in \mathbb{N}$$

where $q = \exp(2i\pi\tau)$.

Def. $\mathscr{L}'$ and $\mathscr{L}$ are isomorphic iff there exists P in $SL_2(\mathbb{Z})$ s.t.

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = P \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Thm. $\mathscr{L}$ and $\mathscr{L}'$ are isomorphic iff $j(\mathscr{L}) = j(\mathscr{L}')$.

Isogenous lattices

Def. $\mathscr{L}$ and $\mathscr{M}$ are isogenous iff $\exists \alpha \in \mathbb{C}, \alpha\mathscr{L} \subset \mathscr{M}$.

Most interesting case: $\mathscr{M}$ is a sublattice of $\mathscr{L}$ s.t. $\mathscr{L}/\mathscr{M}$ is cyclic of finite index. In other words:

$$\mathscr{M} = (a\omega_1 + b\omega_2)\mathbb{Z} + (c\omega_1 + d\omega_2)\mathbb{Z}$$

and $ad - bc = m$ with $\gcd(a,b,c,d) = 1$.

Fundamental theorem (modular polynomial): $\exists \alpha \in \mathbb{C}$ s.t. $\alpha\mathscr{M} \subset \mathscr{L}$ iff $\exists m$ s.t. $\Phi_m(j(\mathscr{M}), j(\mathscr{L})) = 0$ where

$$\Phi_m(X,\tau) = \prod_{A \in \mathscr{S}_m} (X - j(A\tau)) = \sum_{k=0}^{\mu_0(m)} C_k(\tau) X^k,$$

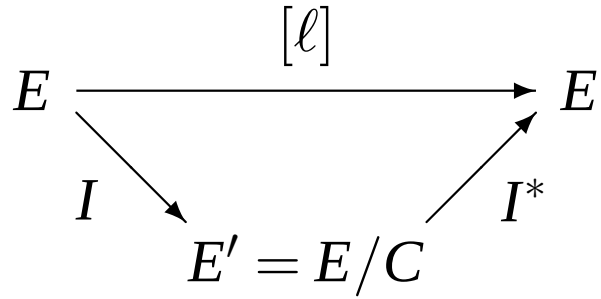
with

$$\mathscr{S}_m = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, ad = m, \gcd(a,b,d) = 1, a > 0, d > b \geq 0 \right\}$$

of cardinality $\mu_0(m) = m \prod_{p|m}(1 + 1/p)$.

SEA again

If j' is any root of $\Phi_\ell(X, j(E))$, then there exists an isogeny between E and $E' = E/C$:



$$I(X,Y) = \left(\frac{k(X)}{h(X)^2}, \ldots\right), \quad \deg(k) = \ell, \deg(h) = (\ell-1)/2$$

$$I(P) = O_E \Leftrightarrow h(X) = 0$$

$$I(P) = O_E \Rightarrow I^*(I(P)) = [\ell]P = O_E$$

$\rightarrow f_\ell(X)$ has a factor of degree $(\ell-1)/2$

Rem. Computing E', I is done via Weiestrass functions, see Bostan/Morain/Salvy/Schost (*Math. Comp.* 2008).

Properties of the modular polynomial

Thm.

- $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$;
- $\Phi_m(Y,X) = \Phi_m(X,Y)$;
- if m is squarefree, then the coefficient of highest degree of $\Phi_m(X,X)$ is ± 1.

Prop. If $(m_1,m_2) = 1$, then

$$\Phi_{m_1 m_2}(X,J) = \mathrm{Resultant}_Z(\Phi_{m_1}(X,Z), \Phi_{m_2}(Z,J)).$$

Prop. If $m = \ell^e$ with $e > 1$, then

$$\Phi_{\ell^e}(X,J) = \mathrm{Resultant}_Z(\Phi_{\ell}(X,Z), \Phi_{\ell^{e-1}}(Z,J))/\Phi_{\ell^{e-2}}(Z,J)^{\ell}.$$

Thm.[Kronecker] If ℓ is prime, then

$$\Phi_\ell(X,Y) \equiv (X^\ell - Y)(Y^\ell - X) \bmod \ell.$$

Numerical examples

$$\Phi_2(X,Y) = X^3 + X^2\left(-Y^2 + 1488\,Y - 162000\right)$$
$$+X\left(1488\,Y^2 + 40773375\,Y + 8748000000\right)$$
$$+Y^3 - 162000\,Y^2 + 8748000000\,Y - 15746400000000.$$

$$\Phi_3(X,Y) = X^4 + Y^4 + 1855425871872000000000X + 452984832000000X^2 + 36864000X^3$$
$$+1855425871872000000000Y - 770845966336000000XY + 8900222976000X^2Y$$
$$-1069956X^3Y + 452984832000000Y^2 + 8900222976000XY^2 + 2587918086X^2Y^2$$
$$+2232X^3Y^2 + 36864000Y^3 - 1069956XY^3 + 2232X^2Y^3 - X^3Y^3.$$

Height

Thm. (P. Cohen)
$H(\Phi_m) = 6\mu_0(m)(\log m - 2\sum_{p|m}(\log p)/p + O(1))$.

ℓ	101	211	503	1009	2003
$H(\Phi_\ell)$	3985	9256	24736	53820	115125
PCohen	2768	6743	18736	41832	91320

Trick: $H \geq \log|\Phi_\ell(0,0)|$ and

$$\Phi_\ell(X,X) = \prod_{x^2 - Df^2 y^2 = 4\ell} H_{-Df^2}(X)^*,$$

where $H_{-Df^2}(X)$ is the Hilbert class polynomial (complex multiplication).

Computing the modular polynomial

Remember that

$$j(q) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n q^n.$$

Then $\Phi_\ell(X, Y)$ is such that $\Phi_\ell(j(q), j(q^\ell))$ vanishes identically.

Naive method: indeterminate coefficients (over $\mathbb{Q}$ or small p's); at least $\tilde{O}((\ell^2)^\omega)$ operations over $\mathbb{Q}$.

Atkin (analysis by Elkies):

1. use q-expansion of j and j with $O(\ell^2)$ terms;
2. compute power sums of roots of Φ_ℓ, write them as polynomials in J;
3. go back to coefficients of $\Phi_\ell(X, J)$ via Newton's formulas;
4. use CRT on small primes. $\tilde{O}(\ell^3 \mathrm{M}(p))$; used for $\ell \leq 1000$ fifteen years ago.

Computing modular polynomials (cont'd)

Charles+Lauter (2005): compute Φ_ℓ modulo p using supersingular invariants mod p, Mestre *méthode des graphes*, ℓ torsion points defined over $\mathbb{F}_{p^{O(\ell)}}$ and interpolation. $\tilde{O}(\ell^4 \mathsf{M}(p))$

Enge (2004); Dupont (2004): use complex floating point evaluation and interpolation. $\tilde{O}(\ell^3)$

Write

$$\Phi_\ell(X,J) = X^{\ell+1} + \sum_{u=0}^{\ell} c_u(J) X^u$$

where $c_u(J) \in \mathbb{Z}[J]$, $\deg(c_u(J)) \leq \ell+1$. All computations are done using precision $H = O(\ell \log \ell)$.

1. **for** $\ell+1$ values of z_i **do**:

   1.1 Compute floating point approximations to the $\ell+1$ roots $j_r(z_i)$ of $\Phi_\ell(X, j(z_i))$ to precision H;

   1.2 Build $\prod_{r=1}^{\ell+1}(X - f_r(z_i)) = X^{\ell+1} + \sum_{u=0}^{\ell} c_u(j(z_i)) X^u$; $O(\mathsf{M}(\ell)\log\ell)$ ops.

2. Perform $\ell+1$ interpolations for the c_u's: $O((\ell+1)\mathsf{M}(\ell)\log\ell)$ ops.

All 1.2 + 2 has cost $O(\ell \mathsf{M}(\ell)(\log\ell)\mathsf{M}(H)) = \tilde{O}(\ell^3)$.

Examples

ℓ	r	H	$\deg(J)$	eval(s)	interp(s)	tot (d)	Mb gz
3011	5	7560	200				368
3079	97	9018	254	7790	640	23	547
3527	13	9894	268	799	1440	3	746
3517	97	10746	290	12400	1110	42	850
4003	13	11408	308	1130	2320	4	1127
5009	5	13349	334	880	3110	3	1819
6029	5	16418	402	1550	6370	7	3251
7001	5	19473	466	2440	11700	13	5182
8009	5	22515	534	3500	20000	22	7905
9029	5	25507	602	5030	33100	35	11460
10079	5	28825	672	7690	56300	61	16152

IV. A glimpse at genus 2

- Points $\longrightarrow$ g-uplet of points on the Jacobian of $y^2 = x^{2g+1} + \cdots$;
- Lattice: $\mathbb{C}/\mathbb{Z}^{2g}$; $\wp(z_1, z_2, \ldots, z_g)$, theta-functions, etc.
- $j \longrightarrow$ many more (3 for $g = 2$).
- Division polynomials $\longrightarrow$ polynomial ideals. $\Rightarrow$ Much harder, heavy computer algebra.
- Modular polynomials: very hard to compute; only Φ_2 known (R. Dupont).

$\Rightarrow$ ask Éric (Schost) and Pierrick (Gaudry) for more!

Conclusions

- Interesting polynomials.
- Need computer algebra everywhere (fast techniques).
- More to be done as g increases.

Complements (if needed!!!)

Oddities

Binary polynomials $\Phi_{pq}(X)$ have $\{-1,0,1\}$ coeffs; exact formula known for $a_{pq}(k)$ (Kaplan, 2007).

Ternary polynomials Φ_{pqr}:

- The smallest n for which $C_n(X)$ has a coeff not ≤ 1 is $n = pqr = 105$ and $a_{105}(7) = a_{105}(41) = -2$.
- Gallot/Moree recent preprint on `arXiv`: If $p < q < r$ are primes s.t.

$$p > 3, \quad q \equiv 2 \bmod p, \quad r \equiv (pq-1)/2 \bmod pq.$$

Put $n = pqr$, $k = (p-1)(qr+1)/2$. Then

$$\{a_n(k-r) = -(p-1)/2, \ldots, a_n(k) = (p+1)/2\} = [-(p-1)/2, (p+1)$$

and for all i, $|a_n(i+1) - a_n(i)| \leq 1$ (jump property).
Ex. $p = 5$, $q = 7$, $r = 17$ yields

$$[-2,-1,0,1,1,2,2,1,0,0,-1,-1,-1,0,1,2,2,3].$$