Other Arithmetic Manifestations of Branched Covers

Noam D. Elkies

- Arithmetic geometry of curves:
  ABC effectively implies Mordell etc.
  via Belyi functions

- Branched covers and towers of modular curves

- Trinomials $x^n + ax^k + b$ with interesting Galois groups

ABC consequences via branched covers

The *ABC conjecture* of Masser and Oesterlé ([Oe], see also Lang [L] and Vojta [V, p.71]) attempts a grand generalization of Fermat's

$$x^n + y^n = z^n.$$

Idea: for large n, a primitive solution of that equation would yield coprime integers $A, B, C > 0$ with $A + B = C$ and each of A, B, C having "lots" of repeated factors. More precisely, the "conductor"

$$N = N(A, B, C) := \prod_{p|ABC} p$$

[NB no multiplicity!] would be $< C^{3/n}$.

The ABC conjecture over $\mathbf{Q}$ asserts:

For each $\epsilon > 0$ there exists $K_\epsilon > 0$ such that

$$N > K_\epsilon C^{1-\epsilon}$$

for any coprime positive integers A, B, C with $A + B = C$. If known for some $\epsilon < 1/4$ with explicit K_ϵ then Fermat is reduced to a finite computation.

But do we believe it? Let's try to disprove it by finding an infinite family of (A, B, C) for which $N \ll C^\theta$ for some $\theta < 1$. For instance, parametrize by. . .

. . . S-units: $A = 1$, $C = 2^m$. So $N < 2C$. $\theta = 1$.

. . . Fermat-Pell equation $x^2 - Dy^2 = 1$:
$A = 1$, $B = Dy^2$, $C = x^2$. So $N < \Delta^{1/2} C$. $\theta = 1$.

. . . elliptic curve $x^3 + y^3 = \Delta z^3$:
$A = x^3$, $B = y^3$, $C = \Delta z^3$. So $N < \Delta^{2/3} C$. $\theta = 1$.

. . . ell. curve $Y^2 = X^4 + \Delta$, i.e. $m^4 + \Delta n^4 = y^2$:
$A = m^4$, $B = \Delta n^4$, $C = y^2$. So $N < \Delta^{3/4} C$. $\theta = 1$.

(These last two examples apparently originate with Szpiro 1990 [Sz].)

Hm. How about more complicated polynomials identities such as

$$(x^2 + 22x + 125)(x^2 + 4x - 1)^2 \; + \; 12^3 x \\ = (x^2 + 10x + 5)^3.$$

Let x be an integer such that $x^2 + 22x + 125$ is say twice a square (Fermat-Pell again), and find that θ is $1/2 + 1/6 + 1/3 \ldots$ which again is 1. What's going on!?

We're parametrizing by a curve $\mathcal{C}$ which is either $\mathbf{P}^1$ with two punctures ($0, \infty$ for S-units, real quadratic conjugates for Fermat-Pell), or an elliptic curve. Regard $(A : B : C)$ as a map from $\mathcal{C}$ to the projective line $A + B = C$. That is, a rational function $f = A/C$ on $\mathcal{C}$. In each case we're exploiting multiple roots of $f = 0$, $f = 1$, $f = \infty$ to obtain repeated primes in A, B, C; also, for twice-punctured $\mathbf{P}^1$, the punctures contribute only a bounded factor to N. So, we want f such that

$$m := \#\left(f^{-1}(\{0, 1, \infty\}) \Big\backslash \{\text{punctures}\}\right)$$

[NB again no multiplicities!] is as small as possible relative to the degree d of f. We have $\theta = m/d$, so we win if $m < d$.

Bad news: the total ramification of f bounds m from below (via the distinction between m and the same count with multiplicity). Using Riemann-Hurwitz to compute the ramification, we find

$$m \geq d + 2 - 2g(\mathcal{C}) - \#(\text{punctures}).$$

So $m \geq d$ in each of our cases.

Note: Except for the punctures, this lower bound on m is in effect an ABC theorem for function fields of curves; this theorem is due to Mason 1983 [M2].

Equality holds iff $0, 1, \infty$ are the only branch points — i.e., iff f is a Belyi function! — and $f^{-1}(0, 1, \infty) \supseteq \{\text{punctures}\}$. Note that this is indeed the case in each of our $\theta = 1$ examples; also for the motivating example where $\mathcal{C}$ is $x^n + y^n = z^n$ with $n > 3$.

Good news: We can use this, together with Belyi's theorem, to prove [E1]: if $\mathcal{C}$ has genus at least 2 then there exists $\epsilon > 0$ such that ABC for that ϵ implies finiteness of $\mathcal{C}(\mathbf{Q})$! Likewise for integral points on elliptic curves, rational approximation to algebraic numbers of degree > 2.

Bad news: Faltings got there first [Fa1,Fa2], not to mention Roth [R] and Mordell-Siegel. And none of them had to assume ABC or any other unproved conjecture!

Still: the implications ABC $\Rightarrow$ Mordell etc. are much simpler; and, they are effective: given $\mathcal{C}$, can effectively find ϵ (namely anything in $(0, 1 - (m/d))$, and then from K_ϵ can compute effectively an upper bound on height of $\mathcal{C}(\mathbf{Q})$ etc. [NB at least for Mordell-Faltings no effective upper bound is known.]

[Worry: what if ABC is finally proved but the proof is much more complicated and also ineffective?. . .]

Branched covers and towers of modular curves

A modular curve is, over $\mathbf{C}$, the quotient of the upper half-plane $\mathcal{H}$ by an arithmetic congruence subgroup of $\mathrm{PSL}_2(\mathbf{R})$. Such curves are defined over $\bar{\mathbf{Q}}$, and are of great importance in number theory and elsewhere. If $H \subset G \subset \mathrm{PSL}_2(\mathbf{R})$ is an inclusion of congruence subgroups then $\mathcal{H}/H$ covers $\mathcal{H}/G$. The cover is unramified except possibly at elliptic points of $\mathcal{H}/G$ and (in the classical case $G \subset \mathrm{PGL}_2(\mathbf{Q})$) cusps. Thus if there are only 3 such points then $\mathcal{H}/G \to \mathcal{H}/G$ is a Belyi cover. There are only finitely many such G, all contained in the list of Takeuchi [T] (1977), but these include some of the most interesting examples.

These all have Galois groups involving nothing more complicated than PGL_2, which however includes A_n, S_n for $n \leq 6$ and "most" of the simple finite groups.

In the classical case of elliptic modular curves, we can use q-expansions at the cusp(s) to find 3-point covers that would be most daunting to find any other way; e.g. $\mathrm{PSL}_2(\mathbf{Z}/p)$ with monodromy elements of exponents $2, 3, p$ for p well into the hundreds. (See [E3]. We earlier showed $\mathrm{X}_0(5)$ which is simple enough to find from the ramification; but don't do $\mathrm{X}_0(239)$ that way!)

For Shimura curves (no cusps), the ramification data is often the simplest way to calculate the covers explicitly. See [E4]. Usually the covers reduce badly at p even though all the monodromy generators have order prime to p (cf. Serre's "Problem" in [S, p.90]).

If N is very large then in general we can't hope to see $X_0(N)$ explicitly. But if N is "smooth" we can still access $X_0(N)$ and its Shimura analogues via towers of modular curves. This is simplest when N is a power of a small prime.

Explicit models for such curves are needed in coding theory: It is known that over finite fields of square order q, suitable modular curves have enough "supersingular points" that their total number of rational points is at least $(\sqrt{q}-1)g$ (Ihara and Tsfasman-Vlăduţ-Zink [I,TVZ], 1981–2), which is asymptotically optimal (Drinfeld-Vlăduţ [DV], 1983). Following Goppa [G], this yields the best linear error-correcting codes known over square fields. To construct and use these codes we need the modular curves explicitly.

EXAMPLES:

$\underline{\mathsf{X}_0(2^k)}$: Let

$$x_1 = \xi(\tau) := 1 + \frac{1}{8}\left(\frac{\eta(\tau)}{\eta(4\tau)}\right)^8,$$

a coordinate for the curve $\mathsf{X}_0(4) \cong \mathsf{Pr}^1$. Then the function field of $\mathsf{X}_0(2^k)$ is generated by $x_1, x_2, \ldots, x_{k-1}$ [where $x_j = \xi(2^{j-1}\tau)$], satisfying the quadratic relations

$$(z_j^2 + 1)(x_{j-1}^2 + 1) = 1, \text{ with } z_j = \frac{x_j + 3}{x_j - 1}.$$

For an odd prime $p = 2a+1$, the supersingular points over the field of p^2 elements are those for which x_1 (and thus each x_j) is a root of the Legendre polynomial P_a.

Over the field of 3^2 elements, even simpler: take $y_j = 1 - x_j^{-1}$ and find

$$y_{j+1}^2 = y_j - y_j^2,$$

with the 2^{k-2} supersingular pts. lying above $y_1 = \infty$. Remarkably, not only can one prove directly that this tower attains the asymptotic maximum of $2g$ points over $\mathbf{F}_9$, without ever identifying it with $\{X_0(2^k) : k \geq 2\}$, but it was actually rediscovered in this way by Garcia and Stichtenoth (1996)!

$\underline{X_0(3^k)}$: Now let

$$x_1 = \xi(\tau) := 1 + \frac{1}{3}\left(\frac{\eta(\tau)}{\eta(9\tau)}\right)^3,$$

a coordinate for the curve $X_0(4) \cong Pr^1$, and $x_j = \xi(3^{j-1}\tau)$. Then the function field of $X_0(3^k)$ is generated by $x_1, x_2, \ldots, x_{k-1}$ with the cubic relations

$$(z_j^3 + 1)(x_{j-1}^3 + 1) = 1, \text{ with } z_j = \frac{x_j + 2}{x_j - 1}.$$

Simplification mod 2: $y_j = 1 - x_j^{-1}$ gives

$$y_{j+1}^3 = y_j^3 + y_j^2 + y_j\,,$$

with the 3^{k-2} supersing.pts. again at infinity. (Also found directly by G.-S. 1996.)

Certain Shimura curves can be obtained by modifying these equations: changing

$$(z_j^2 + 1)(x_{j-1}^2 + 1) = 1$$

in $X_0(2^k)$ to

$$(z_j^2 + 3)(x_{j-1}^2 + 3) = 12$$

yields a Shimura modular curve $\mathcal{X}_0(\wp_2^k)$; changing

$$(z_j^3 + 1)(x_{j-1}^3 + 1) = 1$$

in $X_0(3^k)$ to

$$z_j^3 + x_{j-1}^3 = 1$$

yields a curve $\mathcal{X}_0(\wp_3^k)$. These curves reduce to asymp. optimal towers over the quadratic extensions of residue fields of primes of $\mathbf{Q}(\sqrt{3})$ and $\mathbf{Q}(\cos 2\pi/9)$ respectively.

Moreover, unlike the elliptic modular towers, these Shimura towers are **unramified** above the curves $\mathcal{X}_0(\wp_2^5)$ and $\mathcal{X}_0(\wp_3^4)$ of genus 5, 4 respectively; being towers of cyclic covers, these are also contained in Golod-Šafarevič towers over those two curves.

[Some elliptic or Drinfeld modular curves are contained in towers of ray class fields. Could such towers also be used to improve the lower bounds on $\limsup N_q(g)/g$ for nonsquare q?]

What if there are more than 3 branch points?

In [E4] we computed some cases with 4 branch points using extra information. For instance, $\mathcal{H}/H$ has genus 0, and six of the preimages of the branch points are paired by an involution of that genus-0 curve.

Question: is there a version of "rigidity" etc. that permits the enumeration of covers with $n > 3$ branch points but $n-3$ extra conditions such as these?

Trinomials with interesting Galois groups

Examples: $x^5 - 5x + 12$ has 10-element dihedral Galois group over $\mathbf{Q}$. Gal($x^7 - 7x + 3$) is the simple group of order 168 [Matzat-Trinks 1969].

Problem: for each n, k ($k < n$) and every subgroup $G \subset S_n$, describe trinomials $ax^n + bx^k + c$ with Galois group (contained in) G.

We assume k, n coprime and $k < n/2$. Can ask the question over any field; over $\mathbf{Q}$, the group G must contain an involution with at most 3 fixed points (complex conjugation).

Given n, k, trinomials $ax^n + bx^k + c$ are classified up to scaling by an invariant $F := a^k b^{-n} c^{n-k}$.

Punchline: G-trinomials are parametrized by a curve $\mathcal{C}$ on which F is a 3-point function.

(For the case $k = 1$ see Matzat [M4, II §3]. This was also observed by M.Artin, and probably others.)

Why? Consider first the case of $G = \{\text{id}\}$. Then we're looking for $ax^n + bx^k + c$ to split completely. Let $x_1, \ldots, x_n$ be its roots. Then

$$\sum_{i=1}^{n} x_i^m = 0, \quad 0 < m < n \text{ except } m = n - k.$$

Our $\mathcal{C}$ is then just the complete intersection of these hypersurfaces in $\mathbf{P}^{n-1}$. [Warning: this model is singular if $k > 2$.] It is also the Galois closure of the cover of the F-line obtained by solving $ax^n + bx^k + c$; thus it ramifies only at $F = \infty$, 0, and $(-n)^{-n}k^k(n-k)^{n-k}$. The monodromy elements there have cycle structures (n), $(k)(n-k)$, and $(2)(1)^{n-2}$ respectively.

It is now clear that for general G we take the quotient of that $\mathcal{C}$ by G to obtain the curve parametrizing trinomials with Galois $\subseteq G$. This is still a cover of the F-line ramified at most at the same three points. We can then also calculate the genus of the curve from the ramification of this cover.

In some cases we have been able to calculate explicitly this curve $\mathcal{C}/G$ together with the function F on it. We list several examples in which G is a primitive subgroup of S_n (other than the easy S_n, A_n) with an involution fixing ≤ 3 letters (so that $\mathcal{C}/G$ has real points).

genus zero.

$(n, k) = (5, 1)$: The general such polynomial with Galois group contained in the 20-element subgroup of S_5 (a.k.a. the $aX+b$ group mod 5) is

$$(4u^2 + 16)x^5 + (5u^2 - 5)x + (4u^2 + 10u + 6)$$

Taking $u = t - 1/t$ gives the general polynomial with (at most) dihedral Galois group:

$$\begin{aligned}(2t^2 + 2)^2 x^5 + 5(t^4 - 3t^2 + 1)x \\ + (4t^4 + 10t^3 - 2t^2 - 10t + 4)\end{aligned}$$

either $t = \pm 1$ recovers $X^5 - 5X + 12$ where $X = 2x$.

$(n,k) = (6,1)$: Here we look for the transitive 120- and 60- element subgroups of S_6, obtained from the action of $\mathrm{PGL}_2(\mathbf{Z}/5)$ and $\mathrm{PSL}_2(\mathbf{Z}/5)$ on the projective line mod 5 and isomorphic with S_5, A_5 respectively.

We compute that for the first of these groups the general trinomial is

$$(125-u)x^6+12u(u+3)^2x+u(u-5)(u+3)^2$$

For instance, $u=-1$ yields a trinomial equivalent to x^6-4x^5+336, with Galois group S_5.

To get the general A_5 trinomial of this form, set $u=t^2$ to make the discriminant a square. This yields

$$(125-t^2)x^6+12(t^3+3t)^2x+(t^2-5)(t^3+3t)^2$$

For instance, $t=1$ yields a trinomial equivalent to x^6-6x^5-124, with Galois group A_5.

genus one.

$(n, k) = (5, 2)$: For the 20-element group, $\mathcal{C}$ is an elliptic curve with minimal form

$$y^2 + xy + y = x^3 + x^2 + 35x - 28$$

(15-A4(F) in Cremona [C]), and a degree-6 Belyi function

$$2^2 5^{-5}(9xy - x^3 - 15x^2 - 36x + 32)$$

with monodromy generators of cycle structures $51, 6, 222$.

This curve has rank zero, so there are up to scaling only finitely many irreducible trinomials of the form $x^5 + ax^2 + b$ with solvable Galois group. We list them next:

The group $\mathcal{C}(\mathbf{Q})$ is cyclic of order 8, generated by the quintuple zero $T : (x, y) = (2, 6)$. Excluding this, the simple zero $3T = (32, 171)$, and the origin, leaves 5 points. Three of them are multiples of $2T$ and give a dihedral group:

$$x^5 - 5x^2 - 3, \quad x^5 - 25x^2 - 300, \quad x^5 - 5x^2 + 15.$$

Curiously the first and third of these generate the same field.

The remaining two points are odd multiples of T and give quintic trinomials with the full 20-element Galois group:

$$5x^5 - 10x^2 - 1, \quad x^5 - 100x^2 - 1000.$$

genus two.

$(n,k) = (7,1)$, with G the 168-element group: $\mathcal{C}$ is a curve of genus 2 with model

$$y^2 = x(81x^5+396x^4+738x^3+660x^2+269x+48)$$

and (at least) 7 $\mathbf{Q}$-pts. at $x = 0, -3, 1/9, \infty$. Two $x = -3$ points and one with $x = 1/9$ yield degenerate polynomials; the Weierstrass point $x = 0$ recover the familiar $x^7 - 7x + 3$; the two points at infinity yield $x^7 - 154x + 99$ (also known [EFM]), and the new example

$$37^2x^7 - 154x + 99;$$

and the remaining $x = 1/9$ point yields yet another G-trinomial:

$$499^2x^7 - 23956x + 3^4113.$$

Conjecture: these are all the points of $\mathcal{C}(\mathbf{Q})$, and thus (up to scaling) all the G-trinomials over $\mathbf{Q}$.

$(n, k) = (8, 1)$, with G the 1344-element group $\mathrm{AGL}_3(\mathbf{Z}/2)$: $\mathcal{C}$ is a curve of genus 2 with model

$$y^2 = x^6 + 20x^4 + 12x^3 + 25x^2 + 24x + 16$$

[as simplified by Michael Stoll], with (at least) four rational point pairs, at $x = \infty, 0, 6, -4/3$. Of the 8 points, three, with $x = -4/3, -4/3, 6$, are degenerate. This leaves 5 points, but only four polynomials, because two with $x = 0, \infty$ yield the same F! The resulting polynomial

$$x^8 + 324x + 567$$

has Galois group of order 168: $\mathrm{PSL}_2(\mathbf{Z}/7)$ acting on $\mathbf{P}^1(\mathbf{Z}/7)$. The remaining 3 points with $x = 0, \infty, 6$ yield distinct G-trinomials:

$$x^8 + 168x + 28, \quad x^8 + 576x + 1008,$$

and

$$19^4 53\, x^8 + 19x + 2$$

(Galois gps. checked by B.Poonen on Magma).

Again we conjecture: these are all the points of $\mathcal{C}(\mathbf{Q})$, and thus all the G-trinomials over $\mathbf{Q}$ up to scaling.

Further references:

For $(n,k) = (5,1)$, the general polynomial with 20-element Galois group is given in [M4, p.90-91 (Satz 3)], and attributed there to Weber [W, §189]. The dihedral specialization is calculated in [M4, p.93 (Satz 4)], and attributed to [JRYZ]. For $(n,k) = (6,1)$, Matzat gives the general S_5 and A_5 polynomials in [M4, p.94], and attributed them to Malle [M1], together with the generic trinomials with Galois groups the (imprimitive but) transitive subgroups of S_6 of orders 24, 48, 72, and a specialization with cyclic Galois group $\mathbf{Z}/6$. In [M4, p.95] Matzat also reports on the case $(n,k) = (7,1)$ with 168-element Galois group, but gives the genus as 3 instead of the correct 2.

Remark:

The curves and Belyi functions for $n = 4, 5$ come from suitable elliptic modular curves. This explains the low conductor of the elliptic curves that arise for $(n,k) = (5,2)$.