Finding low degree places on $X_1(N)$

Mark van Hoeij

Florida State University

September 19, 2023

Notation

The following correspond to each other:

- A place P on $X_1(N)/\mathbb{Q}$.
- A discrete valuation $v_P : \mathbb{Q}(X_1(N)) \to \mathbb{Z} \bigcup \{\infty\}$.
- (if P is not a cusp): An elliptic curve E and a point of exact order N, (both defined over the residue field of P).

Denote the degree of the residue field as $\deg(P) = [\mathbb{Q}(P) : \mathbb{Q}]$.

If a function $g \in \mathbb{Q}(X_1(N)) - \mathbb{Q}$ has degree d, then $X_1(N)$ has infinitely many places P of degree d.

Low degree place if P is not a cusp and $\mathbb{Q}(X_1(N))$ has no function of degree $\deg(P)$. (Sporadic torsion is slightly stronger).

E.g. $\deg(P) <$ gonality, the lowest degree in $\mathbb{Q}(X_1(N)) - \mathbb{Q}$.

Degrees of functions and *low degree places* (van Hoeij, 2012)

N	degrees	N	degrees	N	degrees
1–10	1^+	29	*9,10*, 11^+	45	*10,12,14*$^+$, 18, 20^+
11	2^+	30	*5*, 6^+	46	*14*$^+$, 19^+
12	1^+	31	*9*$^+$, 12^+	47	*20*$^+$, 29^+
13–16	2^+	32	8, *9*, 10^+	48	*11,12,14*$^+$, 16, 18^+
17	4^+	33	*7*$^+$, 10, 12^+	49	*14,19*, 21, *22*$^+$, 30^+
18	2^+	34	*8,9*, 10^+	50	*10,12*, 15, *16*$^+$, 20, 22^+
19	5^+	35	*8,10*$^+$, 12, 14^+	51	*15,18*$^+$, 24, 29^+
20	3^+	36	*7*, 8^+	52	*16*$^+$, 21, 24^+
21	*3*, 4^+	37	*6,10,12*$^+$, 18^+	53	*22,25*$^+$, 37^+
22	4^+	38	*10*, 12^+	54	*13,15*$^+$, 18, 20^+
23	7^+	39	*8–10,12*$^+$,14,16^+	55	*18,23*$^+$, 30, 34^+
24	4^+	40	*8*$^+$, 12, 14^+	56	*18*$^+$, 24, 26, 28^+
25	5,*6,7*, 8^+	41	*14,17*$^+$, 22^+	57	*12,16,18,19,21,22,24*$^+$,30,36^+
26	6^+	42	*8*$^+$, 12^+	58	*12,14,16,20*$^+$, 31^+
27	6^+	43	*12,14,15,17*$^+$,24^+	59	*31*$^+$, 46^+
28	*5*, 6^+	44	*11*$^+$, 15^+	60	*13,15*$^+$, 24, 26^+

```
N = 21, found 1 diamond-orbit.
N = 21, degv = 3, degj = 1, j = -140625/8, [x^3-3*x^2+3 = 0, y+x^2-2*x-1 = 0]

N = 25, found 2 diamond-orbits.
N = 25, degv = 6, degj = 3, [x^3-x^2+1 = 0, y^2+(x^2-2*x-1)*y+x = 0]
N = 25, degv = 7, [x^7+x^6-x^5-x^4+x^2+x-1 = 0, y-x^2-x = 0]

N = 28, found 1 diamond-orbit.
N = 28, degv = 5, [x^5-x^4-2*x^3-x^2+2*x+2 = 0, y-x^3+1 = 0]

N = 29, found 3 diamond-orbits.
N = 29, degv = 9, [x^9-8*x^8+23*x^7-26*x^6+2*x^5+17*x^4-11*x^3+2*x^2+1 = 0,
        y-x^8+6*x^7-11*x^6+4*x^5+6*x^4-6*x^3+3*x^2 = 0]
N = 29, degv = 10, degj = 5, [x^10+2*x^8-6*x^7+6*x^6-6*x^5+9*x^4-5*x^3-2*x^2+3*x-1 = 0,
        163*y+328*x^9+188*x^8+724*x^7-1557*x^6+1006*x^5-1129*x^4+2124*x^3-192*x^2-1263*x+437 = 0]
N = 29, degv = 10, [x^10-3*x^9+8*x^7-5*x^6-6*x^5+5*x^4-2*x^2+1 = 0,
        29*y-2*x^9-x^8+11*x^7+8*x^6-49*x^5+77*x^3-35*x^2-46*x+13 = 0]

N = 30, found 2 diamond-orbits.
N = 30, degv = 5, [x^5+x^4-3*x^3+3*x+1 = 0, y-2*x^4-x^3+6*x^2-4*x-4 = 0]
N = 30, degv = 5, [x^5+x^4-7*x^3+x^2+12*x+3 = 0, 53*y-3*x^4-7*x^3-6*x^2-11*x+73 = 0]

N = 31, found 5 diamond-orbits.
N = 31, degv = 9, degj = 3, [x^9-2*x^8+x^6-x^5+14*x^4-28*x^3+19*x^2-2*x-1 = 0,
        119*y-9*x^8+28*x^7-16*x^6-46*x^5+11*x^4-125*x^3+440*x^2-386*x-150 = 0]
N = 31, degv = 10, degj = 1, j = 0, [x^10-4*x^9+3*x^8+6*x^7-2*x^6-8*x^5-8*x^4+11*x^3+6*x^2-5*x+1 = 0,
        215*y-109*x^9+266*x^8+207*x^7-801*x^6-606*x^5+304*x^4+1470*x^3+410*x^2-1000*x-71 = 0]
N = 31, degv = 11, [x^11-x^10+2*x^8+x^6-7*x^5+x^4+4*x^3-x^2+2*x-1 = 0,
  2033*y-1036*x^10+31*x^9+503*x^8-2108*x^7-1676*x^6-2654*x^5+5898*x^4+4556*x^3-2817*x^2-2307*x-3370 = 0]
N = 31, degv = 11, [x^11-2*x^10-6*x^9+8*x^8+9*x^7-x^6-6*x^5-13*x^4-x^3+7*x^2+4*x+1 = 0,
        43*y+61*x^10-144*x^9-319*x^8+596*x^7+370*x^6-131*x^5-311*x^4-690*x^3+123*x^2+291*x+89 = 0]
N = 31, degv = 11, [x^11-8*x^10+23*x^9-25*x^8+8*x^6+14*x^5-10*x^4-8*x^3+10*x^2-5*x+1 = 0,
        329*y-114*x^10+879*x^9-2255*x^8+1444*x^7+2063*x^6-1120*x^5-3115*x^4+524*x^3+2397*x^2-576*x-653 = 0
```

I found almost 4000 diamond-orbits for $N \leq 60$. Before this website and arXiv (2012) very few examples were known (Najman, $N = 21$).

An application: testing Theorems

If you have a conjecture or Theorem about places on $X_1(N)$, test it with examples from my website.

Co-authors of "Sporadic Cubic Torsion" used website to find counter examples to:

Wang (2019), Theorem 1.2,
Wang (2020), Theorem 0.3.

Degrees of functions and *low degree places* (added in 2014)

N	degrees	N	degrees
61	*20,24,26,27,30,31,33*$^+$, 49^+	71	*44,45,47*$^+$, 66^+
62	*22*$^+$, 36^+	72	*22,24*$^+$, 32, 36, 40^+
63	*18,20*$^+$, 36, 39, 41^+	73	*24,30,36,42,46,48*$^+$, 70^+
64	*24*$^+$, 32, 36, 38^+	74	*18,20,29–31,34*$^+$, 51^+
65	*20,24,26,28,30*$^+$, 42, 48^+	75	*25,31–33,35–37,39*$^+$,40,45,50,55,60^+
66	*16,19*$^+$, 30, 32, 35^+	76	*30,35*$^+$, 45, 48, 50, 52, 53, 54, 56^+
67	*22,30,33,37,39,43*$^+$, 58^+	77	*40,48*$^+$, 60, 68, 72^+
68	*26*$^+$, 36, 40, 42^+	78	*24,25,27,28,30*$^+$, 42, 48, 49, 51^+
69	*28,29,32,34,36*$^+$, 44, 54^+	79	*26,42,51,54,57–59,61*$^+$, 82^+
70	*20,24,26*$^+$, 36, 40, 42^+	80	*20,24,28,32,35*$^+$, 48, 54, 56^+

Entry $N = 71$: The notation 66^+ indicates that $X_1(71)$ has functions of degree d for any $d \geq 66$. To prove that, I'll explain how to quickly find functions of degrees $66, \ldots, 2 \times 66 - 1$.

After that I'll explain how places of degrees *44, 45, 47–65* were found. (For $N > 60$ the website only lists one example for each N, d)

Cusps and modular units

Cusps of $X_1(N)$ $=$ poles of $j : X_1(N) \to \mathbb{P}^1$.

The $\mathbb{Q}$-conjugacy classes of the cusps are denoted $C_0, \ldots, C_{\lfloor N/2 \rfloor}$.

The residue field of C_i is a subfield of $\mathbb{Q}(\zeta_N)$ of degree $\gcd(i, N)$ (divide by 2 and round up if $i = 0$ or $i = N/2$).

For example, $\deg(C_1) = 1$ for any N.

Cusp-sums $\sum n_i C_i$ with $\sum n_i \cdot \deg(C_i) = 0$ represents element of

$$J_1(N)(\mathbb{Q})_{\text{cusp}} \subseteq J_1(N)(\mathbb{Q})_{\text{tors}} \subseteq J_1(N)(\mathbb{Q})$$

Important for proofs: If $N \leq 55$ and $N \neq 37, 43, 53, 54$ then all three are equal.

We quickly find $J_1(N)(\mathbb{Q})_{\text{cusp}}$ by computing all modular units (functions with support $\subseteq$ {cusps}).

Cusps and modular units

The paper Gonality of the modular curve $X_1(N)$ (joint with *Maarten Derickx*) gives a conjectured basis of modular units.

Marco Streng proved the conjecture in Generators of the group of modular units for $\Gamma_1(N)$ over the rationals.

A Divisor Formula and a Bound on the $\mathbb{Q}$-gonality of the Modular Curve $X_1(N)$ (joint with *Hanson Smith*) gives explicit divisors.

Let $L = \mathrm{SPAN}(\mathrm{div}(F_2), \ldots, \mathrm{div}(F_{\lfloor N/2 \rfloor}))$.

(`cusp_divisors_program` on my website computes this)

Identify L with a submodule of $\mathbb{Z}^n$ with $n = 1 + \lfloor N/2 \rfloor$.

Example $N = 71$. Repeatedly running LLL(L)

$\rightsquigarrow$ elements $v = (n_0, n_1, \ldots, n_{\lfloor N/2 \rfloor}) \in L$

$\rightsquigarrow$ modular units g_v of degree $|v| := \sum \max(0, n_i) \cdot \deg(C_i)$

$\rightsquigarrow$ functions of degree $66, 67, 68, 69, 70, \ldots$

After that: only interested in places of degree < 66.

Running LLL

Recall: divisors(modular units) are stored in $L \subset \mathbb{Z}^n$.

We repeatedly apply the LLL algorithm to L. Each LLL run uses another randomly chosen metric on $\mathbb{Z}^n$ (so that we don't find the same vectors over and over again).

To prove that $X_1(71)$ has a function of every degree ≥ 66, find v's in L with $|v| = \deg(g_v) = 66, 67, \ldots 2 \times 66 - 1$.

Idea: Modify LLL code to store $|v|$ for every vector encountered (not just the output vectors).

Quickly proves that $X_1(71)$ has modular units of any degree ≥ 66.

Next: find and store places of degree < 66.

Finding low degree places

Each $v = (n_0, n_1, \ldots) \in L$ encodes a modular unit g_v of degree $|v|$. If $|v|$ is in the desired range, use linear algebra to find $g_v = \prod F_j^{m_j}$ where $F_2, \ldots, F_{\lfloor N/2 \rfloor + 1} = \text{basis(modular units)}$.

If $r \in \mathbb{Q}$, consider the roots of $g_v - r$.

- If $r = 0$ then all roots are cusps.
- If r is random, then $\mathrm{roots}(g_v - r)$ is likely a place of degree d (not a low-degree place).

Let C_i be a cusp for which $n_i = 0$, i.e. $C_i \notin \mathrm{support}(g_v)$.

Formulas in paper with Hanson Smith $\rightsquigarrow$ dominant term of $F_j(C_i)$ $\rightsquigarrow$ fast computation for $r := g_v(C_i)$.

Having C_i as root lowers the degree of the remaining roots:

$$\mathrm{roots}(g_v - r) - \{C_i\} \text{ has only places of degree } < d.$$

Often $r = \pm 1$. (Can improve "often" to "always" if you want).

Boosting "often" to "always"

If C_i is a cusp, then we can define $L_i := \{v \in L \mid g_v(C_i) = \pm 1\}$.

Could also define $L_{i,i}$ ($g_v \pm 1$ has at least a double root at C_i), etc.

For any $v \in L_i$ (find such v with modified LLL), the corresponding modular unit g_v has value ± 1, so $g_v - 1$ or $g_v + 1$ already has a forced root.

$\rightsquigarrow$ lowers the potential degrees of the remaining roots
$\rightsquigarrow$ high probability of finding low degree places, if they exist.

Could also try more than one forced root (search $L_i \bigcap L_j$) and/or a forced double root (search $L_{i,i}$), etc.

Even without such improvements, the $\mathrm{roots}(g \pm 1)$-method is very effective; experiments with a more rigorous approach (Riemann-Roch computations) did not yield anything new.

Computing roots efficiently (only needed for large N)

Write $\mathbb{Q}(X_1(N)) \cong \mathbb{Q}(x)[y]/(F_N)$ where F_N is a defining equation.

To find roots$(g-1)$, compute the norm $N(g-1) \in \mathbb{Q}(x)$.

If we know all poles of $g-1$ (and some roots), then we can write $N(g-1) = AB/C$ with $A, B, C \in \mathbb{Q}[x]$, and B, C known.
The x-coordinates of the remaining roots of g are roots of A.

Idea: No need to spell out g in terms of coordinates x, y. It suffices to evaluate g at points over finite fields. Then A mod p is recovered by polynomial interpolation, and A is recovered with rational number reconstruction.

If $g = \prod F_i^{m_i}$, can rapidly evaluate each factor F_i at a point with the recurrence for division polynomials.

Defining equations, division polynomials

The following correspond

- A non-cuspidal place of $X_1(N)$.
- (Elliptic curve, point of order N) up to equivalence.
- (j, X) where X is a coordinate of an order-N point on E_j.
- Tate coordinates (b, c).
- Sutherland coordinates (x, y).

$E_j =$ an equation of an elliptic curve with j-invariant j.

$X =$ coordinate of a point on E_j of order $N \rightsquigarrow$ an equation F_N.

For any $N \geq 2$, F_N is

- a defining equation for $X_1(N)$
- a division polynomial (they satisfy recurrence relations)
- (after a small modification) a modular unit on $X_1(N')$, for any $N' \neq N$.

Defining equations, division polynomials

F_N is a defining equation for $X_1(N)$ for $N \geq 2$.

Problem: F_N is very large in (j, X) coordinates.

Solution: Switch to Sutherland coordinates (x, y) if $N \geq 10$, or Tate coordinates (b, c) if $N \geq 4$.

Let $k, N \geq 2$. If $k \neq N$ then:

- $F_k = 0$ (encodes: exact order k)
- $F_N = 0$ (encodes: exact order N)

are mutually contradictory.

This implies: Every root of F_k in $X_1(N)$ is a cusp.
A minor modification (poles) turns F_k into a modular unit.
Basis(modular units) $= \{F_2, \ldots, F_{\lfloor N/2 \rfloor + 1}\}$.

Recurrence relations (converted to (x, y)-coordinates, website)
$\rightsquigarrow$ fast algorithm to evaluate F_k, or to construct $F_k \in \mathbb{Q}[x, y]$.

More rigorous search of low degree places

For $N = 31$. Found 5 diamond-orbits of low degree places, with degrees $9, 10, 11, 11, 11$. Are there more?

Say P is such a place.

$P - \deg(P) \cdot C_1 \rightsquigarrow$ an element of $J_1(31)(\mathbb{Q}) = J_1(31)_{\mathrm{cusps}}$.

The latter is computed explicitly (implementation on my website) and is isomorphic to $\mathbb{Z}/(10) \times \mathbb{Z}/(1772833370)$.

Trying every element (a Riemann-Roch computation for each case) provably produces all low-degree places.

An improvement

Take for instance $N = 31$ and $d = 11$. Found three diamond orbits for N, d with the roots$(g \pm 1)$-method. Are there more?

$J_1(31)(\mathbb{Q}) \hookrightarrow J_1(31)(\mathbb{F}_2)$

$X_1(31)(\mathbb{F}_2)$ has 15 places of degree 1,
0 of degree 2, 3, or 4,
3 of degree 5,
15 of degree 6,
15 of degree 7,
30 of degree 8,
50 of degree 9,
94 of degree 10, and
210 of degree 11.

Taking sums produces $\approx 250,000$ divisors of degree 11.
Take one per diamond-orbit and check if it lifts to $J_1(31)(\mathbb{Q})$.
$\rightsquigarrow$ far fewer cases than previous slide.

Additional improvements

Idea from gonality paper with Maarten Derickx:

If $D = D_1 + C_i = D_2 + C_j$ then D "dominates" both D_1 and D_2.

If we increase degree(D) then
$\implies$ it dominates more divisors D_i
$\implies$ we need fewer Riemann Roch computations.

If we increase degree(D) too much:
$\implies$ dim(RR Space) increases (bad, how to pick right element?)

After some work: Number of Riemann Roch computations $\ll$ number of divisors that need to be covered.

A complication $N = 37$

$J_1(37)(\mathbb{Q}) \cong J_1(37)(\mathbb{Q})_{\text{cusps}} \oplus \mathbb{Z}$.

If D is a divisor, let $\mathrm{index}(D)$ be its image in $\mathbb{Z}$.

Let P_6 be the degree 6 place on $X_1(37)$ from arXiv 2012.
index(P_6) $\neq 0$ (P_6 is not cuspidal).
Assume index(P_6) $= 1$.

LLL($\{v \in L \mid g_v(P_6) = \pm 1\}$) $\rightsquigarrow$ places, index -1 (probabilistic).
Like before, could do a rigorous search for any fixed index $i \in \mathbb{Z}$.

Would like to cover every $N \leq 40$. However, problem at $N = 37$:
To provably find all low-degree places P, need to bound index(P).

(Website has low-degree places with index -1, 0, and 1).

Unrelated conjecture, but related to modular functions??

Gauss Hypergeometric Function ${}_2F_1(a, b\,;c \mid x)$.

Goal: for which $a, b, c \in \mathbb{Q}$ does there exist algebraic functions f, r with $f \neq x$, and with $r \cdot {}_2F_1(a, b\,;c \mid f)$ and ${}_2F_1(a, b\,;c \mid x)$ having same minimal differential equation.

Found some non-trivial examples where $\exists$ such r, f.
For other cases, how to prove such r, f do not exist?

Idea: if $f \in \mathbb{Q}((x))$ has infinitely many primes in denominators, then f is not algebraic over $\mathbb{Q}(x)$.

For prime p to NOT appear in the denominator, a certain congruence needs to hold.

Testing(congruence) $\rightsquigarrow$ a number of conjectures.

A conjecture and a question for the audience

Let $n \geq 3$ and let

$$Y(x) = {}_2F_1(\frac{1}{4} - \frac{1}{2n}, \frac{1}{4} + \frac{1}{2n}; 1 \mid x)^2 \cdot \frac{3n^2+4}{8n^2}\sqrt{1-x}.$$

Let c_p be the coefficient of x^p in the series of $1/Y(x)$ at $x = 0$.

Then for all but finitely many primes p

$$c_p \equiv 1 \mod p \iff p \equiv \pm 1 \mod n.$$

For $n = 3, 4, 6$ this can be proved in multiple ways. Those ${}_2F_1$ functions are related to modular functions (inverse of j-invariant).

Are other cases $n = 5, 7, 8, \ldots$ related to modular functions?

Need a strategy to prove that the congruence $c_p \equiv 1$ mod p holds only for specific primes ($p \equiv \pm 1$ mod n). Where to start?