CHAPTER 2

Gonality of the modular curve $X_1(N)$

GONALITY OF THE MODULAR CURVE $X_1(N)$

MAARTEN DERICKX AND MARK VAN HOEIJ

Abstract. In this paper we compute the gonality over $\mathbb{Q}$ of the modular curve $X_1(N)$ for all $N \leqslant 40$ and give upper bounds for each $N \leqslant 250$. This allows us to determine all N for which $X_1(N)$ has infinitely points of degree d where d is either 5 or 6. We conjecture that the modular units of $\mathbb{Q}(X_1(N))$ are freely generated by $f_2, \ldots, f_{\lfloor N/2 \rfloor + 1}$ where f_k is obtained from the equation for $X_1(k)$.

1. Introduction

Notation 1. *If K is a field, and C/K is a curve*[1]*, then $K(C)$ is the function field of C over K. The gonality $\mathrm{Gon}_K(C)$ is $\min\{\deg(f) \mid f \in K(C) - K\}$. In this article we are interested in the case $C = X_1(N)$, and K is either $\mathbb{Q}$ or $\mathbb{F}_p$.*

It was shown in [Der12] that if $C/\mathbb{Q}$ is a curve and p is a prime of good reduction of then:

$$\mathrm{Gon}_{\mathbb{F}_p}(C) \leqslant \mathrm{Gon}_{\mathbb{Q}}(C). \tag{1}$$

A similar statement was given earlier in [Fre94] which attributes it to [Deu42]. We use (1) only for $C = X_1(N)$. The primes of good reduction of $X_1(N)$ are the primes $p \nmid N$.

The main goal in this paper is to compute $\mathrm{Gon}_{\mathbb{Q}}(X_1(N))$ for $N \leqslant 40$. The $\mathbb{Q}$-gonality for $N \leqslant 22$ was already known [Sut12, p. 2], so the cases $23 \leqslant N \leqslant 40$ are of most interest. For each N, it suffices to:

- Task 1: Compute a basis of $\mathrm{div}(\mathcal{F}_1(N))$, which denotes the set of divisors of modular units over $\mathbb{Q}$, see Definition 1 in Section 2 for details.
- Task 2: Use LLL techniques to search $\mathrm{div}(\mathcal{F}_1(N))$ for the divisor of a non-constant function g_N of lowest degree.
- Task 3: Prove (for some prime $p \nmid N$) that $\mathbb{F}_p(X_1(N)) - \mathbb{F}_p$ has no elements of degree $< \deg(g_N)$. Then (1) implies that the $\mathbb{Q}$-gonality is $\deg(g_N)$.

[1]In this paper, a *curve* over a field K is a scheme, projective and smooth of relative dimension 1 over $\mathrm{Spec}\, K$ that is geometrically irreducible.

Table 1: $\mathrm{Gon}_{\mathbb{Q}}(X_1(N))$ for $N \leqslant 40$. Upper bounds for $N \leqslant 250$.

N	1	2	3	4	5	6	7	8	9	10
gon $=$	1	1	1	1	1	1	1	1	1	1
N	11	12	13	14	15	16	17	18	19	20
gon $=$	2	1	2	2	2	2	4	2	5	3
N	21	22	23	24	25	26	27	28	29	30
gon $=$	4	4	7	4	5	6	6	6	11	6
N	31	32	33	34	35	36	37	38	39	40
gon $=$	12	8	10	10	12	8	18	12	14	12
N	41	42	43	44	45	46	47	48	49	50
gon $\leqslant$	22	12	24	15	18	19	29	16	21	15
N	51	52	53	54	55	56	57	58	59	60
gon $\leqslant$	24	21	37	18	30	24	30	31	46	24
N	61	62	63	64	65	66	67	68	69	70
gon $\leqslant$	49	36	36	32	42	30	58	36	44	36
N	71	72	73	74	75	76	77	78	79	80
gon $\leqslant$	66	32	70	51	40	45	60	42	82	48
N	81	82	83	84	85	86	87	88	89	90
gon $\leqslant$	54	58	90	48	72	64	70	60	104	48
N	91	92	93	94	95	96	97	98	99	100
gon $\leqslant$	84	66	80	83	90	56	123	63	90	60
N	101	102	103	104	105	106	107	108	109	110
gon $\leqslant$	133	72	139	84	96	105	150	72	156	90
N	111	112	113	114	115	116	117	118	119	120
gon $\leqslant$	114	96	167	90	132	105	126	120	144	96
N	121	122	123	124	125	126	127	128	129	130
gon $\leqslant$	132	139	140	120	125	96	211	112	154	126
N	131	132	133	134	135	136	137	138	139	140
gon $\leqslant$	225	120	180	156	144	144	246	132	253	144
N	141	142	143	144	145	146	147	148	149	150
gon $\leqslant$	184	189	210	128	210	184	168	171	291	120
N	151	152	153	154	155	156	157	158	159	160
gon $\leqslant$	299	180	216	180	240	168	323	234	234	184
N	161	162	163	164	165	166	167	168	169	170
gon $\leqslant$	264	162	348	210	240	240	365	192	260	216
N	171	172	173	174	175	176	177	178	179	180
gon $\leqslant$	270	231	392	210	240	240	290	274	420	192
N	181	182	183	184	185	186	187	188	189	190
gon $\leqslant$	429	252	310	264	342	240	360	276	288	270
N	191	192	193	194	195	196	197	198	199	200
gon $\leqslant$	478	224	488	328	336	252	508	240	519	240
N	201	202	203	204	205	206	207	208	209	210
gon $\leqslant$	374	382	420	288	420	398	396	336	450	288
N	211	212	213	214	215	216	217	218	219	220
gon $\leqslant$	583	351	420	396	462	288	480	445	444	360
N	221	222	223	224	225	226	227	228	229	230
gon $\leqslant$	504	342	651	384	360	444	675	360	687	396
N	231	232	233	234	235	236	237	238	239	240
gon $\leqslant$	480	420	711	336	552	435	520	432	748	384
N	241	242	243	244	245	246	247	248	249	250
gon $\leqslant$	761	396	486	465	504	420	630	480	574	375

Tasks 1–3 are only possible when:

(a) There is a modular unit g_N of degree $\mathrm{Gon}_{\mathbb{Q}}(X_1(N))$.
(b) There is a prime $p \nmid N$ for which $\mathrm{Gon}_{\mathbb{F}_p}(X_1(N)) = \mathrm{Gon}_{\mathbb{Q}}(X_1(N))$.

We have completed Tasks 1–3 for $1 < N \leqslant 40$, and hence (a),(b) are true in this range. We do not know if they hold in general.

We implemented two methods for Task 1. Our webpage [DvH] gives the resulting basis of $\mathrm{div}(\mathcal{F}_1(N))$ for $N \leqslant 300$. For Task 2, for each $4 \leqslant N \leqslant 300$ we searched $\mathrm{div}(\mathcal{F}_1(N))$ for short[2] vectors, and placed the best function we found, call it g_N, on our webpage [DvH]. The degree of any non-constant function is by definition an upper bound for the gonality. Table 1 gives $\deg(g_N)$ for $N \leqslant 250$.

Finding the shortest vector in a $\mathbb{Z}$-module is NP-hard. For large N, this forced us to resort to a probabilistic search (we randomly scale our vectors, apply an LLL search, and repeat). So we can not prove that every g_N on our webpage is optimal, even if we assume (a).

For certain N (e.g. $N = p^2$, see Section 4) there are other ways of finding functions of low degree. Sometimes a good function can be found in a subfield of $\mathbb{Q}(X_1(N))$ over $\mathbb{Q}(X_1(1))$, see [DvH]. All low degree functions we found with these methods were also found by our probabilistic LLL search. So the upper bounds in Table 1 are likely sharp when (a) holds (Question 1 in Section 2.2).

At the moment, our only method to prove that an upper bound is sharp is to complete Task 3, which we have done for $N \leqslant 40$. The computational cost of Task 3 increases drastically as a function of the gonality. Our range $N \leqslant 40$ contains gonalities that are much higher than the previous record, so in order to perform Task 3 for all $N \leqslant 40$ it was necessary to introduce several new computational ideas.

Upper bounds (Tasks 1 and 2) will be discussed in Section 2, and lower bounds (Task 3) in Section 3. We cover $N = 37$ separately (Theorem 1), this case is the most work because it has the highest gonality in our range $N \leqslant 40$. Sharp lower bounds for other $N \leqslant 40$ can be obtained with the same ideas. Our computational proof (Task 3) for each $N \leqslant 40$ can be verified by downloading the Magma files from [DvH].

Remark 1. *For each $N \leqslant 40$, the $\mathbb{Q}$-gonality happened to be the $\mathbb{F}_p$-gonality for the smallest prime $p \nmid N$. That was fortunate because the computational complexity of Task 3 depends on p.*

We can not expect the $\mathbb{F}_p$-gonality to equal the $\mathbb{Q}$-gonality for every p. For example, consider the action of diamond operator $<12>$ on $\mathbb{C}(X_1(29))$. The fixed field has index 2 and genus 8 (type: `GammaH(29,[12]).genus()` *in Sage). By Brill-Noether theory, this subfield contains a function f_{BN} of degree $\leqslant \lfloor (8+3)/2 \rfloor = 5$. Viewed as element of $\mathbb{C}(X_1(29))$, its degree is $\leqslant 2 \cdot 5$ which is less than the $\mathbb{Q}$-gonality[3] 11. By*

[2]We want vectors with small 1-norm because $\deg(g) = \frac{1}{2}||\mathrm{div}(g)||_1$.

[3]We do not know if there are other $N \leqslant 40$ with $\mathbb{C}$-gonality $\neq$ $\mathbb{Q}$-gonality.

Chebotarev's theorem, there must then be a positive density of primes p for which the $\mathbb{F}_p$-gonality of $X_1(29)$ is less than 11.

2. Modular equations and modular units

Definition 1. *A non-zero element of $\mathbb{Q}(X_1(N))$ is called a* modular unit *(see* [KL81]*) when all its poles and roots are cusps. Let $\mathcal{F}_1(N) \subset \mathbb{Q}(X_1(N))^*/\mathbb{Q}^*$ be the group of modular units mod $\mathbb{Q}^*$.*

There are $\lfloor N/2 \rfloor + 1$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of cusps, denoted[4] *as $C_0, \ldots, C_{\lfloor N/2 \rfloor}$. Let*

$$\mathcal{D}_1(N) := \mathbb{Z}C_0 \oplus \cdots \oplus \mathbb{Z}C_{\lfloor N/2 \rfloor}$$

be the set of $\mathbb{Q}$-rational cuspidal divisors. The degree[5] *of $\sum n_i C_i$ is $\sum n_i \deg(C_i)$. Denote $\mathcal{D}_1^0(N)$ as the set of cusp-divisors of degree 0, and*

$$\mathcal{C}_1(N) := \mathcal{D}_1^0(N)/\mathrm{div}(\mathcal{F}_1(N)),$$

a finite group called the cuspidal class group*.*

Let E be an elliptic curve over a field K, and P be a point on E of order exactly N. If $N \geqslant 4$ and $\mathrm{char}(K) \nmid N$, one can represent the pair (E, P) in *Tate normal form:*

$$Y^2 + (1-c)XY - bY = X^3 - bX^2, \quad \text{with the point } (0,0). \tag{2}$$

This representation is unique and hence b, c are functions on pairs (E, P). The function field $K(X_1(N))$ is generated by b, c. Whenever we use the notation b or c, we implicitly assume $N \geqslant 4$, because the reduction to (2) succeeds if and only if $N \geqslant 4$. This implies (for $N \geqslant 4$) that poles of b, c must be cusps. The discriminant of (2) is $\Delta := b^3 \cdot (16b^2 + (1 - 20c - 8c^2)b + c(c-1)^3)$ so E degenerates when $\Delta = 0$. So all roots of Δ (and hence of b) are cusps. Poles of Δ, b are cusps because poles of b, c are cusps. So Δ, b are modular units, and hence

$$F_2 := b^4/\Delta \;=\; \frac{b}{16b^2 + (1 - 20c - 8c^2)b + c(c-1)^3} \quad \text{and} \quad F_3 := b$$

are modular units as well.

For $N \geqslant 4$, the functions b, c on $X_1(N)$ satisfy a polynomial equation $F_N \in \mathbb{Z}[b, c]$, namely (for $N = 4, 5, 6, 7, \ldots$) $\;c,\;\; b - c,\;\; c^2 + c - b,\;\; b^2 - bc - c^3, \ldots$

If $k \neq N$, the condition that the order of P is k is incompatible with the condition that the order is N. This, combined with the observation that all poles of b, c are

[4]Let $d|N$, $0 \leqslant i < d$, with $\gcd(i, d) = 1$ and let j be such that the point $P_{d,i,j} = (i, \zeta_N^j)$ has order N in the Neron d-gon $\mathbb{Z}/d\mathbb{Z} \times \mathbb{G}_m$. Let $C_{d,i,j}$ be the cusp corresponding to $P_{d,i,j}$, then $C_{d,i,j}$ and $C_{d',i',j'}$ are in the same Galois orbit iff $d = d'$ and $i \equiv \pm i' \bmod d$. We denote the Galois orbit of $C_{d,i,j}$ as C_n where $0 \leqslant n \leqslant N/2$ and $n \equiv \pm iN/d \bmod N$. With this numbering, the diamond operator $\langle i \rangle$ sends C_n to $C_{n'}$ where $n' \equiv \pm ni \bmod N$.

[5]The degree of C_i is as follows. Let $d = \gcd(i, N)$. If $i \in \{0, N/2\}$ then $\deg(C_i) = \lceil \phi(d)/2 \rceil$, otherwise $\deg(C_i) = \phi(d)$, where ϕ is Euler's function.

cusps, implies (for $N, k \geqslant 4$) that the *modular equation* F_k is a *modular unit* for $X_1(N)$. We define a subgroup of $\mathcal{F}_1(N)$ generated by *modular equations*[6]:

$$\mathcal{F}_1'(N) := < F_2, F_3, \ldots, F_{\lfloor N/2 \rfloor + 1} > \subseteq \mathcal{F}_1(N).$$

Conjecture 1. *$\mathcal{F}_1'(N) = \mathcal{F}_1(N)$ for $N \geqslant 3$. In other words, $\mathcal{F}_1(N)$ is freely generated by modular equations $F_2, \ldots, F_{\lfloor N/2 \rfloor + 1}$.*

We verified this for $N \leqslant 100$, see also Section 2.1. The conjecture holds for $N = 3$ because F_2 rewritten to j, x_0 coordinates generates $\mathcal{F}_1(3)$. The case $N = 2$ is a little different, clearly F_2 can not generate $\mathcal{F}_1(2)$ since it must vanish on $X_1(2)$. However, rewriting F_2F_4 to j, x_0 coordinates produces a generator for $\mathcal{F}_1(2)$. The conjecture is only for $\mathbb{Q}$; if $X_1(N)_K$ has more than $\lfloor N/2 \rfloor + 1$ Galois orbits of cusps, for example $X_1(5)_K$ with $K = \mathbb{C}$ or $K = \mathbb{F}_{11}$, then the rank of $\mathcal{F}_1'(N)$ would be too low.

2.1. **Computations.** As N grows, the size of F_N grows quickly. Sutherland [Sut12] obtained smaller equations by replacing b, c with other generators of the function field. For $6 \leqslant N \leqslant 9$, use r, s defined by

$$r = \frac{b}{c},\ s = \frac{c^2}{b-c},\quad b = rs(r-1),\ c = s(r-1)$$

and for $N \geqslant 10$, use x, y defined by

$$x = \frac{s-r}{rs-2r+1},\ y = \frac{rs-2r+1}{s^2-s-r+1},\quad r = \frac{x^2y-xy+y-1}{x(xy-1)},\ s = \frac{xy-y+1}{xy}.$$

The polynomial defining $X_1(N)$ is then written as $f_4 := c$, $f_5 := b - c$, $f_6 := s - 1$, $f_7 := s - r$, $f_8 := rs - 2r + 1$, $f_9 := s^2 - s - r + 1$, $f_{10} := x - y + 1$, $f_{11} := x^2y - xy^2 + y - 1$, $f_{12} := x - y$, $f_{13} := x^3y - x^2y^2 - x^2y + xy^2 - y + 1$, etc. Explicit expressions for $f_{10}, \ldots, f_{189} \in \mathbb{Z}[x, y]$ can be downloaded from Sutherland's website `http://math.mit.edu/~drew/X1_altcurves.html`.

The same website also lists upper bounds for the gonality for $N \leqslant 189$, that are often sharp when N is prime. Table 1 improves this bound for every composite $N > 26$, a few composite $N < 26$, but only three primes: 31, 67, and 101. When N is prime, we note that Sutherland's [Sut12] bound, $\deg(x)$, equals $[11N^2/840]$ where

[6]An equation is called a modular equation for $X_1(k)$ if it corresponds to P having order k. A computation is needed to show that F_2, F_3 are modular equations in this sense. The fact that F_2 and F_3 correspond to order 2 and 3 is obscured by the b, c coordinates, so we introduce j, x_0 coordinates for $X_1(N)$ that apply to any $N > 1$ provided that $j \notin \{0, 1728\}$. Here x_0 is the x-coordinate of a point P on $y^2 = 4x^3 - 3j(j-1728)x - j(j-1728)^2$. The condition that P has order 2 or 3 can be expressed with equations $\tilde{F}_2, \tilde{F}_3 \in \mathbb{Q}[j, x_0]$. These $\tilde{F}_2, \tilde{F}_3$ are functions on $X_1(N)$ for any $N > 1$. Hence they can (for $N > 3$) be rewritten to b, c coordinates. To obtain modular units, we have to ensure that all poles and roots are cusps, which requires an adjustment: $F_2 := \tilde{F}_2^2/(j^2(j-1728)^3)$ and $F_3 := \tilde{F}_3^3/\tilde{F}_2^4$.

the brackets denote rounding to the nearest integer ($[11N^2/840]$ is a valid upper bound for any $N > 6$, but it is not very sharp for composite N's).

Let $f_2 := F_2$ and $f_3 := F_3$. Then $F_k/f_k \in < f_2, \dots, f_{k-1} >$ for each $k \geqslant 2$. In particular

$$\mathcal{F}_1'(N) = < f_2, f_3, \dots f_{\lfloor N/2 \rfloor + 1} > .$$

For each $3 \leqslant N \leqslant 300$ and $2 \leqslant k \leqslant \lfloor N/2 \rfloor + 1$ we calculated $\mathrm{div}(f_k) \in \mathcal{D}_1(N)$. This data can be downloaded (in row-vector notation) from our webpage [DvH]. This data allows one to determine $\mathcal{D}_1^0(N)/\mathrm{div}(\mathcal{F}_1'(N))$ for $N \leqslant 300$. If that is $\cong \mathcal{C}_1(N)$, then the conjecture holds for N. We tested this by computing $\mathcal{C}_1(N)$ with Sage[7] for $N \leqslant 100$. The $\mathrm{div}(f_k)$-data has other applications as well:

Example 1. *Let $N = 29$. Suppose one wants to compute explicit generators for the subfield of index 2 and genus 8 mentioned in Remark 1. Let $\tilde{x}, \tilde{y}$ denote the images of x, y under the diamond operator <12>. Clearly $\tilde{x}x$, $\tilde{y}y$ are in our subfield, which raises the question: How to compute $\tilde{x}, \tilde{y}$?*

Observe that $x = f_7/f_8$ and $y = f_8/f_9$ (The relations $1-x = f_5f_6/(f_4f_8)$, $1-y = f_6f_7/f_9$, $1-xy = f_6^2/f_9$ may be helpful for other examples.) So we can find $\mathrm{div}(x)$ *by subtracting the (7-1)'th and (8-1)'th row-vector listed at* [DvH] *for $N = 29$. We find $(0, -1, -2, -3, -1, 0, 0, 0, 3, 2, -1, -3, 2, 3, 1)$ which encodes* $\mathrm{div}(x) =$

$$-C_1 - 2C_2 - 3C_3 - C_4 + 3C_8 + 2C_9 - C_{10} - 3C_{11} + 2C_{12} + 3C_{13} + C_{14}.$$

The diamond operator <12> sends C_i to $C_{\pm 12i \bmod N}$ and hence $\mathrm{div}(\tilde{x}) =$

$$2C_1 - C_4 - 2C_5 + C_6 - 3C_7 + 2C_8 + 3C_9 - C_{10} + 3C_{11} - C_{12} - 3C_{13}.$$

Since $\mathrm{div}(f_2), \dots, \mathrm{div}(f_{15})$ *are listed explicitly at* [DvH]*, solving linear equations provides $n_2, \dots, n_{15}$ for which* $\mathrm{div}(\tilde{x}) = \sum n_i \mathrm{div}(f_i)$. *Setting* $g := \prod f_i^{n_i} =$

$$\frac{(x^2y - xy + y - 1)(x-1)^2(x - y + 1)(x^2y - xy^2 - x^2 + xy - x + y - 1)^4y^3}{(y-1)^2(xy-1)(x-y)(x^2y - xy^2 - xy + y^2 - 1)^4x^4},$$

it follows that $\tilde{x} = cg$ for some constant c (c is not needed here, but it can be determined easily by evaluating $\tilde{x}$ and g at a point.) Repeating this computation for y, we find explicit expressions for $\tilde{x}x$, $\tilde{y}y$. An algebraic relation can then be computed with resultants; it turns out that $\tilde{x}x$, $\tilde{y}y$ generate the subfield.

2.2. **Explicit upper bound for the gonality for $N \leqslant 40$.** The following table lists for each $10 < N \leqslant 40$ a function of minimal degree. We improve the upper bound from Sutherland's website (mentioned in the previous section) in 16 out of these 30 cases.

11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
x	x	x	x	x	y	x	h_1	x	x	h_1	x	x	h_1	h_2
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
y	h_3	h_3	x	h_5	h_1	h_4	h_6	h_1	h_7	h_8	x	h_2	h_9	h_5

[7]The $\mathbb{Z}$-module of modular units is computed with modular symbols by determining the $\sum n_i c_i \in \mathbb{Z}^{\mathrm{cusps}}$ of degree 0 with $\sum n_i \{c_i, \infty\} \in H_1(X_1(N)(\mathbb{C}), \mathbb{Z}) \subset H_1(X_1(N)(\mathbb{C}), \mathbb{Q})$.

Here

$$h_1 = \frac{x^2y - xy^2 + y - 1}{(x-y)x^2y}, \quad h_2 = \frac{x(1-y)(x^2y - xy^2 - xy + y^2 - 1)}{(x-y+1)(x^2y - xy^2 + y - 1)},$$
$$h_3 = \frac{(1-x)(x^2y - xy^2 - xy + y^2 - 1)}{(x-y)(x^2y - xy^2 + y - 1)}, \quad h_4 = \frac{(1-x)(x^2y - xy^2 + y - 1)}{x(1-y)},$$
$$h_5 = \frac{(1-y)(x^2y - xy^2 - xy + y^2 - 1)}{(x-y)y(x-y+1)}$$
$$h_6 = \frac{f_{10}f_{11}f_{12}}{f_{17}}, \quad h_7 = \frac{f_{17}}{f_{18}}, \quad h_8 = \frac{f_{14}f_{17}^2}{f_{19}^2}, \quad h_9 = \frac{f_{12}f_{13}f_{14}}{f_{19}}.$$

Each $h_1, \ldots, h_9$ is in the multiplicative group $< f_2, f_3, \ldots >$. To save space, we only spelled out $h_1, \ldots, h_5$ in x, y-notation (the f_{19} that appears in h_9 is substantially larger than the f_{11} that appears in h_1). Similar expressions for $N \leqslant 300$ are given on our website [DvH].

Question 1. *Does $\mathbb{Q}(X_1(N))$ always contain a modular unit of degree equal to the $\mathbb{Q}$-gonality?*

It does not suffice to restrict to rational cusps (C_i's of degree 1) because then $N = 36$ would be the first counter example. Question 1 may seem likely at first sight, after all, it is true for $N \leqslant 40$. However, we do not conjecture it because the function $f_{\mathrm{BN}} \in \mathbb{C}(X_1(29))$ from Remark 1 is not a modular unit over $\mathbb{C}$, but unlike Conjecture 1, there is no compelling reason to restrict Question 1 to $\mathbb{Q}$.

3. Lower bound for the gonality

Task 3 is equivalent to showing that the Riemann-Roch space $H^0(X_1(N), D)$ is $\mathbb{F}_p$ for every divisor $D \geqslant 0$ of degree $< \deg(g_N)$. This is a finite task, because over $\mathbb{F}_p$, the number of such D's is finite. For $N = 37$, the $\mathbb{Q}$-gonality is 18, and the number of D's over $\mathbb{F}_2$ with $D \geqslant 0$ and $\deg(D) < 18$ is far too large to be checked one by one on a computer. So we will need other methods to prove:

Theorem 1. *Let $f \in \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$. Then $\deg(f) \geqslant 18$.*

Definition 2. *Let $f \in K(X_1(N))$. The support $\mathrm{Supp}(\mathrm{Div}(f))$ is $\{P \in X_1(N)_K \mid v_P(f) \neq 0\}$, i.e., the set of places where f has a non-zero valuation (a root or a pole). Let $\mathrm{mdeg}_K(f)$ denote $\max\{\deg_K(P) \mid P \in \mathrm{Supp}(\mathrm{Div}(f))\}$. Likewise, if $D = \sum n_i P_i$ is a divisor, then $\mathrm{mdeg}_K(D) := \max\{\deg_K(P_i) \mid n_i \neq 0\}$.*

Overview of the proof of Theorem 1:
We split the proof in two cases: Section 3.2 will prove Theorem 1 for the case $\mathrm{mdeg}(f) = 1$. Section 3.3 will introduce notation, and prove Theorem 1 for the case $\mathrm{mdeg}(f) > 1$. (Task 3 for the remaining $N \leqslant 40$ is similar to Section 3.3 but easier, and will be discussed in Section 3.4.)

3.1. **The $\mathbb{F}_2$ gonality of $X_1(37)$.** In [Der12] there are already tricks for computing the $\mathbb{F}_p$ gonality of a curve in a computationally more efficient way than the brute force method from earlier papers. These tricks were not efficient enough to compute the $\mathbb{F}_2$ gonality of $X_1(37)$. However, by subdividing the problem, treating one part with lattice reduction techniques, and the other part with tricks from [Der12], the case $N = 37$ becomes manageable on a computer. We divide the problem as follows:

Proposition 1. *If there is a $g \in \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ with $\deg(g) \leqslant 17$ then there is an $f \in \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ with $\deg(f) \leqslant 17$ that satisfies at least one of the following conditions:*

1. $\mathrm{mdeg}(f) = 1$
2. *all poles of f are rational cusps, and f has $\geqslant 10$ distinct poles.*
3. *f has a pole at $\geqslant 5$ rational cusps and at least one non-rational pole.*

Proof. $X_1(37)$ has 18 $\mathbb{F}_2$-rational places, all of which are cusps. View g as a morphism $X_1(37)_{\mathbb{F}_2} \to \mathbb{P}^1_{\mathbb{F}_2}$. For all $h \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_2})$ we have $\deg(g) = \deg(h \circ g)$. If there is $h \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_2})$ such that $\mathrm{mdeg}(h \circ g) = 1$ then take $f = h \circ g$ and we are done. Now assume that such h does not exist. Then at least two of the three sets $g^{-1}(\{0\}), g^{-1}(\{1\}), g^{-1}(\{\infty\})$ contain a non-rational place. If all three do, then the one with the most rational cusps has at least $18/\#\mathbb{P}^1(\mathbb{F}_2) = 6 > 5$ rational cusps and we can take $f = h \circ g$ for some $h \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_2})$. Otherwise we can assume without loss of generality that $g^{-1}(\{\infty\})$ only contains rational cusps. If $g^{-1}(\{\infty\})$ contains at least 10 elements then we can take $f = g$. If $g^{-1}(\{\infty\})$ contains at most 9 elements then $g^{-1}(\{0\}) \cup g^{-1}(\{1\})$ contains at least $18 - 9 = 9$ rational cusps, so either $g^{-1}(\{0\})$ or $g^{-1}(\{1\})$ contains at least 5, and we can take $f = 1/g$ or $f = 1/(1-g)$. □

3.2. **The case $N = 37$ and mdeg = 1.**

Proposition 2. *Every $f \in \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ with $\mathrm{mdeg}(f) = 1$ has $\deg(f) \geqslant 18$.*

Proof. Let $M = \mathbb{Z}^{X_1(37)(\mathbb{F}_2)} \subset \mathrm{Div}(X_1(37)_{\mathbb{F}_2})$ be the set of all divisors D with $\mathrm{mdeg}(D) = 1$. Let $N = \ker(M \to \mathrm{Pic}\, X_1(37)_{\mathbb{F}_2})$, i.e. principal divisors in M. Magma can compute N directly from its definition, an impressive feat considering the size of the equation! First download the file `X1_37_AFF.m` from our web-page [DvH]. It contains the explicit equation for $X_1(37)$ over $\mathbb{F}_2$, and assigns it to `AFF` with the Magma command AlgorithmicFunctionField.

```
> load "X1_37_AFF.m";
> plc1 := Places(AFF, 1); //18 places of degree 1, all cusps.
> M := FreeAbelianGroup(18);  gen := [M.i : i in [1..18]];
> ClGrp, m1, m2 := ClassGroup(AFF); //takes about 3 hours.
> N := Kernel(Homomorphism(M, ClGrp, gen, [m2(i) : i in plc1]));
```

Let $\|\_\|_1$ and $\|\_\|_2$ be the standard 1 and 2 norm on M with respect to the basis $X_1(37)(\mathbb{F}_2)$ (i.e. `plc1`). For a divisor $D \in N$ with $D = \mathrm{Div}(g)$ we have $\deg(g) =$

$\frac{1}{2}\|D\|_1$. So we need to show that N contains no non-zero D with $\|D\|_1 \leqslant 2 \cdot 17$. The following calculation shows that N contains no divisors $D \neq 0$ with $\|D\|_2^2 \leqslant 2(14^2+3^2) = 410$ and $\frac{1}{2}\|D\|_1 \leqslant 17$.

```
> //Convert N to a more convenient data-structure.
> N := Lattice(Matrix( [Eltseq(M ! i) : i in Generators(N)] ));
> SV := ShortVectors(N,410);
> Min([&+[Abs(i) : i in Eltseq(j[1])]/2 : j in SV]);
18 1
```

From this we can conclude two things. First, there is a function f of degree 18 with $\mathrm{mdeg}(f) = 1$. We already knew that from our LLL search of $\mathrm{div}(\mathcal{F}_1(37))$, but this is nevertheless useful for checking purposes (see Remark 2 below). Second, if there is a non-constant function f of degree $\leqslant 17$ and $\mathrm{mdeg}(f) = 1$ then $\|\mathrm{Div}\, f\|_2^2 > 2(14^2+3^2)$ so either f or $1/f$ must have a pole of order $\geqslant 15$ at a rational point. Then either f or $1/f$ is in a Riemann-Roch space $H^0(X_1(N)_{\mathbb{F}_2}, 15p+q+r)$ with p, q, r in $X_1(37)(\mathbb{F}_2)$. Since the diamond operators act transitively on $X_1(37)(\mathbb{F}_2)$ we can assume without loss of generality that p is the first element of $X_1(37)(\mathbb{F}_2)$ returned by Magma. The proof of the proposition is then completed with the following computation:

```
> p := plc1[1];
> Max([Dimension(RiemannRochSpace(15*p+q+r)) : q,r in plc1]);
1 1
```

□

Remark 2. *Computer programs could have bugs, so it is reasonable to ask if Magma really did compute a proof of Proposition 2. The best way to check this is with independent verification, using other computer algebra systems.*

We computed $\mathrm{div}(f_k)$*, for* $k = 2, \ldots, \lfloor 37/2 \rfloor + 1$*, in Maple with two separate methods. One is based on determining root/pole orders by high-precision floating point evaluation at points close to the cusps. The second method is based on Puiseux expansions. The resulting divisors are the same. Next, we searched the* $\mathbb{Z}$*-module spanned by these divisors for vectors with a low 1-norm. Maple and Magma returned the same results, but what is important to note is that this search (in characteristic 0) produced the same vectors as the divisors of degree-18 functions (in characteristic 2) that Magma found in the computation for Proposition 2.*

We made similar checks throughout our work. Magma's RiemannRochSpace command never failed to find a function whose existence was known from a computation with another computer algebra system. The structure of Magma's ClassGroup also matched results from computations in Sage and Maple.

The key programs that the proofs of our lower bounds depend on are Magma's RiemannRochSpace program (needed for all non-trivial N*'s), and ClassGroup program (needed for* $N = 37$*). We have thoroughly tested these programs, and are confident that they compute correct proofs.*

3.3. **The case $N = 37$ and mdeg > 1.** It remains to treat cases 2 and 3 of Proposition 1. Let $S_2 \subseteq \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ be the set of all functions f with $\deg(f) \leqslant 17$ such that all poles of f are rational and f has at least 10 distinct poles. Similarly let $S_3 \subseteq \mathbb{F}_2(X_1(37)) - \mathbb{F}_2$ be the set of all functions f with $\deg(f) \leqslant 17$ such that f has a pole at at least 5 distinct rational points and a pole at at least 1 non-rational point. To complete the proof of Theorem 1 we need to show:

Proposition 3. *The sets S_2 and S_3 are empty.*

We will prove this with Magma computations, using ideas similar to those in [Der12]. The main new idea is in the following definition:

Definition 3. *Let C be a curve over a field $\mathbb{F}$ and $S \subseteq \mathbb{F}(C) - \mathbb{F}$ a set of non-constant functions. We say that a set of divisors $A \subset \operatorname{Div} C$* dominates *$S$ if for every $f \in S$ there is a $D \in A$ such that $f \in \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \operatorname{Aut}(C)$ (i.e. $f = g \circ f' \circ h$ for some $g \in \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}})$, $f' \in H^0(C, D)$, and $h \in \operatorname{Aut}(C)$).*

It follows directly from this definition that

$$S \subseteq \bigcup_{D \in A} \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \operatorname{Aut}(C)$$

and hence:

Proposition 4. *Let C be a curve over a field $\mathbb{F}$, $S \subseteq \mathbb{F}(C) - \mathbb{F}$ and $A \subset \operatorname{Div} C$. Suppose that A dominates S, and that:*

$$\forall_{D \in A}\ S \cap \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \operatorname{Aut}(C) = \emptyset. \tag{3}$$

Then $S = \emptyset$.

Proof of Proposition 3. Appendix A.1 gives two sets A_2 and A_3 that dominate S_2 and S_3 respectively. The Magma computations given there show that

$$\forall_{D \in A_2 \cup A_3} \min\{\deg(f) \mid f \in H^0(C, D) - \mathbb{F}_2\} \geqslant 18$$

where $C = X_1(37)_{\mathbb{F}_2}$. Since $\deg(f)$ is invariant under the actions of $\operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}})$ and $\operatorname{Aut}(C)$ it follows (for $i = 2, 3$ and $D \in A_i$) that $S_i \cap \operatorname{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \operatorname{Aut}(C) = \emptyset$ so we can apply Proposition 4. □

3.4. **The cases $N \leqslant 40$ and $N \neq 37$.** Subdividing the problem into three smaller cases as in Proposition 1 was not necessary for the other $N \leqslant 40$. Instead we used an easier approach which is similar to the case $N = 37$ and mdeg > 1.

For an integer N let p_N denote the smallest prime p such that $p \nmid N$. Let $d_N = \deg(g_N)$ denote the degree of the lowest degree function we found for N (Section 2.2 or online [DvH]). Now in order to prove $\operatorname{Gon}_{\mathbb{Q}}(X_1(N)) \geqslant d_N$ we will prove $\operatorname{Gon}_{\mathbb{F}_{p_N}}(X_1(N)) \geqslant d_N$. We have done this by applying Proposition 4 directly with S the set of all functions of degree $< d_N$. To verify hypothesis (3) from Proposition 4 with a computer for $A = \operatorname{Div}^+_{d_N - 1}(X_1(N)_{\mathbb{F}_{p_N}})$ (i.e. all effective divisors of degree $d_N - 1$) was unfeasible in a lot of cases. Instead we used the following

proposition to obtain a smaller set A of divisors that still dominates all functions of degree $< d_N$.

Proposition 5. *Let C be a curve over a finite field $\mathbb{F}_q$ and d an integer. Let $n := \lceil \#C(\mathbb{F}_q)/(q+1) \rceil$ and*

$$D = \sum_{p \in C(\mathbb{F}_q)} p$$

then

$$A := \mathrm{Div}^+_{d-n}(C) + D = \left\{ s' + D \mid s' \in \mathrm{Div}^+_{d-n}(C) \right\}$$

dominates all functions of degree $\leqslant d$.

Proof. For all $f \colon C \to \mathbb{P}^1_{\mathbb{F}_q}$ we have $f(C(\mathbb{F}_q)) \subseteq \mathbb{P}^1(\mathbb{F}_q)$. By the pigeon hole principle, there is a point p in $\mathbb{P}^1(\mathbb{F}_q)$ whose pre-image under f has at least n points in $C(\mathbb{F}_q)$. Moving p to ∞ with a suitable $g \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}_q})$, the function $g \circ f$ has at least n distinct poles in $C(\mathbb{F}_q)$. So if $\deg(f) \leqslant d$ then $\mathrm{Div}(g \circ f) \geqslant -s - D$ for some $s \in \mathrm{Div}^+_{d-n}(C)$. □

Proposition 5 reduces the number of divisors to check, but increases their degrees. However, for our case $C = X_1(N)$ the gonality is generally much lower then the genus, so the Riemann-Roch spaces from equation (3) are still so small that it is no problem to enumerate all their elements, and compute their degrees to show $S \cap \mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}}) H^0(C, D) \,\mathrm{Aut}(C) = \emptyset$.

As a further optimization we can make A even smaller by using the orbits under diamond operators. The Magma computations [DvH] show that hypothesis (3) in Proposition 4 is satisfied for S, the set of functions of degree $< d_N$ in $\mathbb{F}_{p_N}(X_1(N)) - \mathbb{F}_{p_N}$, and A, an explicit set of divisors dominating S.

Despite all our tricks to reduce the number of divisors, the number of divisors for $N = 37$ (due to its high gonality) remained far too high for our computers, specifically, divisors consisting of rational places. We handled those by using the relations between rational places in the Jacobian. That idea (worked out in Section 3.2) allowed us to complete $N = 37$ and thus all $N \leqslant 40$.

4. Patterns in the gonality data

Definition 4. *Let $\Gamma \subseteq \mathrm{PSL}_2(Z)$ be a congruence subgroup and $X(\Gamma) := \mathbb{H}^*/\Gamma$ be the corresponding modular curve over $\mathbb{C}$. The* improvement factor *of a function $f \in \mathbb{C}(X(\Gamma)) - \mathbb{C}$ is the ratio*

$$[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma] / \deg(f) = \deg(j) / \deg(f).$$

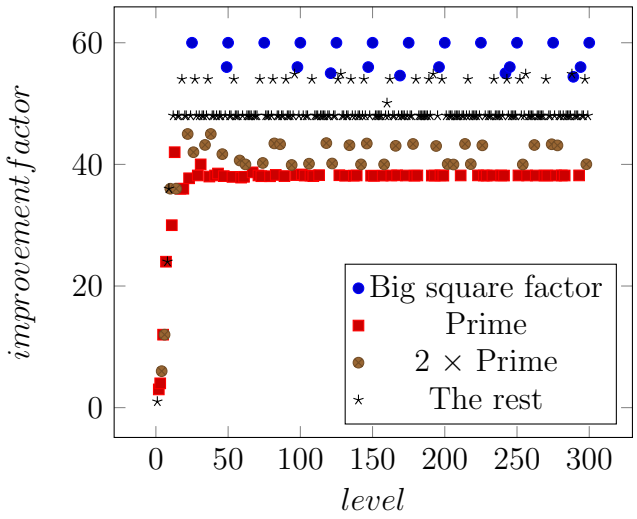
The definition is motivated by a well known bound from Abramovich:

Theorem 2 ([Abr96])**.**

$$\mathrm{Gon}_{\mathbb{C}}(X(\Gamma)) \geqslant \frac{7}{800} [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma].$$

If Selbergs eigenvalue conjecture is true then $7/800$ can be replaced by $1/96$.

The theorem says that an improvement factor can not exceed 800/7, for any Γ, even over $\mathbb{C}$. To compare this with $X_1(N)$ (over $\mathbb{Q}$), we plotted the improvement factors of our g_N's from [DvH]. This revealed a remarkable structure:



What immediately pops out is that our best improvement factor is often 48 (in 151 out of 300 levels N). Levels $N > 9$ with an improvement factor < 48 are either of the form $N = p$ or $N = 2p$ for a prime p. For prime levels, our improvement factor converges to 420/11.

Levels of the form $N = kp^2$ with $p > 3$ prime stand out in the graph, with improvement factors significantly higher than 48. To explain this, first observe that improvement factors for kp^2 are $\geqslant$ those of p^2 because:

Remark 3. *If $\Gamma \subseteq \Gamma'$ are two congruence subgroups, $\pi : X(\Gamma) \to X(\Gamma')$ denotes the quotient map and $f \in \mathbb{C}(X(\Gamma'))$ then f and $f \circ \pi$ have the same improvement factor. So improvement factors for $X(\Gamma')$ can not exceed those for $X(\Gamma)$.*

It remains to explain the high observed improvement factors at levels $N = p^2$:

level	5^2	7^2	11^2	13^2	17^2
improvement	60	56	55	$54\frac{3}{5}$	$54\frac{2}{5}$

The best (lowest degree, highest improvement factor) modular units g_N we found for these five cases turned out to be invariant under a larger congruence subgroup $\Gamma_0(p^2) \cap \Gamma_1(p) \supseteq \Gamma_1(p^2)$. Now

$$\Gamma_0(p^2) \cap \Gamma_1(p) = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma(p) \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}^{-1}.$$

This suggests to look at $X(p)$ to find high improvement factors for $X_1(p^2)$.

5. Points of degree 5 and 6 on $X_1(N)$

The values of N for which the curve $X_1(N)$ has infinitely many places of degree d over $\mathbb{Q}$ are known for $d = 1$ (Mazur), $d = 2$ [K86], $d = 3$ [JKL11a] and $d = 4$ [JKL11b]. In this section, we extend this to $d = 5$ and $d = 6$.

Theorem 3. *$X_1(N)$ has infinitely many places of degree $d = 5$ resp. $d = 6$ over $\mathbb{Q}$ if and only if*

- *for $d = 5$: $N \leqslant 25$ and $N \neq 23$.*
- *for $d = 6$: $N \leqslant 30$ and $N \neq 23, 25, 29$.*

The case $X_1(25)$ is by far the most interesting (and the most work) because its set of non-cuspidal places of degree $d = 6$ is finite[8] even though 6 is larger than the $\mathbb{Q}$-gonality of $X_1(25)$! The remainder of this section contains the proof of Theorem 3 and a remark on larger d's.

Lemma 1.

(1) *Let $C/\mathbb{Q}$ be a curve. If C has a function f over $\mathbb{Q}$ of degree d then C has infinitely many places of degree d over $\mathbb{Q}$.*
(2) *If the Jacobian $J(C)(\mathbb{Q})$ is finite, then the converse holds as well. To be precise, if C has more than $\#J(C)(\mathbb{Q})$ places of degree d, then $\mathbb{Q}(C)$ contains a function of degree d.*
(3) *If $N \leqslant 60$ and $N \neq 37, 43, 53, 57, 58$ then $J_1(N)(\mathbb{Q})$ is finite.*
(4) *If $N > 60$ or $N = 37, 43, 53, 57, 58$ then $X_1(N)$ has finitely many places of degree $\leqslant 6$.*

Proof. (1) Hilbert's irreducibility theorem shows that there are infinitely many places of degree d among the roots of $f - q = 0$, $q \in \mathbb{Q}$.

(2) If $n = \#J(C)(\mathbb{Q}) < \infty$ and $P_1, \ldots, P_{n+1}$ are distinct places of degree d, then by the pigeon hole principle, there exist $i \neq j$ with $P_i - P_1 \sim P_j - P_1$. The function giving this linear equivalence has degree d.

(3) Magma has a provably correct algorithm to determine if $L(J_1(N), 1)$ is 0 or not. It shows $L(J_1(N), 1) \neq 0$ for each N in item 3. By a result of Kato this implies that $J_1(N)(\mathbb{Q})$ has rank zero and hence is finite.

(4) The case $N = 58$ follows from the map $X_1(58) \to X_1(29)$ and the fact that $X_1(29)$ has only finitely many points of degree $\leqslant 6$ (by items 3, 2 and Table 1). $\mathrm{Gon}_{\mathbb{Q}}(X_1(37)) = 18$, and a similar computation shows $\mathrm{Gon}_{\mathbb{Q}}(X_1(43)) \geqslant 13$ (this bound is not sharp, but the computational effort increases if we try to prove a better bound). For $N = 53, 57$ or > 60, we find $\frac{7}{800}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] > 12$, and Abramovich's bound (Section 4) implies $\mathrm{Gon}_{\mathbb{Q}}(X_1(N)) \geqslant 13$. Now item 4 follows from the main theorem of [Fre94] which states that a curve $C/\mathbb{Q}$ with $C(\mathbb{Q}) \neq \emptyset$ has finitely many places of degree $< \mathrm{Gon}_{\mathbb{Q}}(C)/2$. □

[8] and not empty, we found an explicit example [DvH]

Items 4, 3, 2, and 1 of Lemma 1 reduce Theorem 3 step by step to:

Proposition 6. *$X_1(N)$ has a function over $\mathbb{Q}$ of degree $d = 5$ resp. $d = 6$ if and only if:*

- *for $d = 5$: $N \leqslant 25$ and $N \neq 23$.*
- *for $d = 6$: $N \leqslant 30$ and $N \neq 23, 25, 29$.*

Proof. For each N, d listed here, our divisor data [DvH] makes it easy to find an explicit function in $\mathcal{F}_1(N)$ (Section 2) of degree d. So it suffices to show that there are no such functions in the other cases.

- $N > 40$ and $N \neq 42$: In these cases $\frac{7}{800}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] > 6$, so it follows from Abramovich's bound (Section 4).
- $N \leqslant 40$ or $N = 42$ and $(N, d) \neq (25, 6)$: For $N \leqslant 40$ see Table 1. A similar computation (Proposition 5 with $q = 5$, $d = 6$) shows $\mathrm{Gon}_{\mathbb{Q}}(X_1(42)) > 6$.
- $(N, d) = (25, 6)$: We prove this by verifying conditions 1–5 of Proposition 7 below with $C = X_1(25)$, $d = 6$ and $p = 2$.
  1. The rank of $J_1(25)(\mathbb{Q})$ is 0 and $\#J_1(25)(\mathbb{F}_3) = 2503105$ is odd. So $\#J_1(25)(\mathbb{Q})$ is finite and odd and hence $J_1(25)(\mathbb{Q}) \hookrightarrow J_1(\mathbb{F}_2)$.

  2,3 We verified this using a Magma computation (files at [DvH]).

  4. Since $6 - \mathrm{Gon}_{\mathbb{F}_2} X_1(25) = 1$ we only need to show surjectivity of $W_5^1(\mathbb{Q}) \to W_5^1(\mathbb{F}_2)$. A Magma computation shows $\#W_5^1(\mathbb{F}_2) = 1$, and $W_5^1(\mathbb{Q}) \neq \emptyset$ by Table 1.
  5. This is true because $X_1(25)(\mathbb{F}_2)$ consists exactly of the 10 cusps that come from the rational cusps in $X_1(25)(\mathbb{Q})$.

□

For $N \leqslant 40$, applying a `ShortVectors`-search to our divisor data [DvH] shows that $\mathbb{Q}(X_1(N))$ has a function of degree $d \geqslant \mathrm{Gon}_{\mathbb{Q}}(X_1(N))$ if $(N, d) \notin S = \{(25, 6), (25, 7), (32, 9), (33, 11), (35, 13), (39, 15), (40, 13)\}$. The search also showed that there are no modular units with $(N, d) \in S$. Ruling out degree-d functions other than modular units is more work:

Proposition 7. *Let $C/\mathbb{Q}$ with $C(\mathbb{Q}) \neq \emptyset$ be a smooth projective curve with good reduction at a prime p. Let $W_d^r(K)$ denote the closed subscheme of $\mathrm{Pic}^d C(K)$ corresponding to the line bundles $\mathcal{L}$ of degree d whose global sections form a K-vectorspace of dimension $\geqslant r + 1$. Suppose that:*

(1) *$J(C)(\mathbb{Q}) \to J(C)(\mathbb{F}_p)$ is injective.*
(2) *$\mathbb{F}_p(C)$ contains no functions of degree d.*
(3) *$W_d^2(\mathbb{F}_p) = \emptyset$.*
(4) *$W_{d-i}^1(\mathbb{Q}) \to W_{d-i}^1(\mathbb{F}_p)$ is surjective for all $1 \leqslant i \leqslant d - \mathrm{Gon}_{\mathbb{F}_p}(C)$.*
(5) *$C^{(i)}(\mathbb{Q}) \to C^{(i)}(\mathbb{F}_p)$ is surjective for all $1 \leqslant i \leqslant d - \mathrm{Gon}_{\mathbb{F}_p}(C)$.*

Then $\mathbb{Q}(C)$ contains no functions of degree d.

Proof. Item 1 and $C(\mathbb{Q}) \neq \emptyset$ imply that $\mathrm{Pic}^k C(\mathbb{Q})$ to $\mathrm{Pic}^k C(\mathbb{F}_p)$ is injective for all k. To show that $\mathbb{Q}(C)$ has no function of degree d it suffices to show for all $\mathcal{L}$ in $W_d^1(\mathbb{Q})$ that every 2-dimensional subspace $V \subset \mathcal{L}(C)$ has a base point.

Let $\mathcal{L} \in W_d^1(\mathbb{Q})$. Item 3 implies $\dim_{\mathbb{F}_p} \mathcal{L}_{\mathbb{F}_p}(C_{\mathbb{F}_p}) = 2$ and so $\dim_{\mathbb{Q}} \mathcal{L}(C) = 2$. Let $D_{\mathbb{F}_p}$ be the divisor of basepoints of $\mathcal{L}_{\mathbb{F}_p}$ and let i be its degree. Item 2 implies $i \geqslant 1$ and because $\mathcal{L}_{\mathbb{F}_p}(-D_{\mathbb{F}_p}) \in W_{d-i}^1(\mathbb{F}_p)$ we have $i \leqslant d - \mathrm{Gon}_{\mathbb{F}_p}(C)$. By item 5 there is a $D \in C^{(i)}(\mathbb{Q})$ that reduces to $D_{\mathbb{F}_p}$. By the injectivity of $\mathrm{Pic}^{d-i} C(\mathbb{Q}) \to \mathrm{Pic}^{d-i} C(\mathbb{F}_p)$, we know that $\mathcal{L}(-D)$ is the unique point lying above $\mathcal{L}_{\mathbb{F}_p}(-D_{\mathbb{F}_p})$. Then item 4 gives the following inequalities

$$2 \leqslant \dim_{\mathbb{Q}} \mathcal{L}(-D)(C) \leqslant \dim_{\mathbb{Q}} \mathcal{L}(C) = 2.$$

In particular, the unique 2-dimensional $V \subset \mathcal{L}(C)$ has the points in D as base points. □

Remark 4. *To extend Theorem 3 to $d = 7, 8$, we can use the same mathematical arguments; the main difficulty is computational. Our Magma files for Proposition 7 cover $(N, d) = (25, 6)$ and $(25, 7)$. Our divisor data* [DvH] *makes it easy*[9] *to find functions of degree 7 on $X_1(N)$ for $N = 1 \ldots 24, 26, 27, 28, 30$ and functions of degree 8 for $N = 1 \ldots 28, 30, 32, 36$. To prove that these are the only values for which $X_1(N)$ has infinitely many points of degree 7 resp. 8, we need to compute higher lower-bounds for the gonality, specifically*[10] *for $N = 42, 43, 53$ (for $d = 7$) and $N = 42, 43, 44, 46, 48, 53, 57$ (for $d = 8$). For $d = 7$, the lower-bound needed for Frey's theorem is 15, which is 3 less than the bound we managed to compute in Theorem 1. So the number of Riemann Roch spaces needed for $d = 7$ is manageable, however, each Riemann Roch computation for $N = 53$ will likely be slow (we did not attempt this). For $d = 8$, the number of Riemann Roch computations will be much higher.*

New mathematical problems arise for $d = 9$. $X_1(37)$ has a Jacobian with positive rank, and the $\mathbb{Q}$-gonality is 18 so we can not use Frey's theorem to rule out infinitely many places of degree 9. $J_1(37)$ has only one simple abelian sub-variety of positive rank, namely an elliptic curve E isogenous to $X_0^+(37)$. So the question whether $X_1(37)$ has infinitely many places of degree 9 is equivalent to the question whether $W_9^0(X_1(37))$ contains a translate of E. Higher values of d lead to additional mathematical problems, for instance, when $X_1(N)$ has infinitely many places of degree d but no function of degree d.

Appendix A. Magma Calculations

We use one custom function. It takes as input a divisor and gives as output the degrees of all non-constant functions in the associated Riemann-Roch space.

[9] This part takes little CPU time and can easily be done for much larger (N, d)'s.

[10] All but finitely many values of N are handled by an improvement to Abramovich's bound (Remark 4.5 in [BGGP05]) and $N = 58$ is again handled by its map to $X_1(29)$.

```
function FunctionDegrees(divisor)
    constantField := ConstantField(FunctionField(divisor));
    space,map := RiemannRochSpace(divisor);
    return [Degree(map(i)) : i in space | map(i) notin constantField];
end function;
```

We divide the computation according to *type*:

Definition 5. *Write D as*

$$\sum_{i=1}^{k} n_i p_i$$

with p_i distinct places and $n_i \in \mathbb{Z} - \{0\}$ such that $(\deg(p_1), n_1) \geqslant (\deg(p_2), n_2) \geqslant \cdots \geqslant (\deg(p_k), n_k)$ where $\geqslant$ is the lexicographic ordering on tuples. Then type(D) is defined to be the ordered sequence of tuples

$$((\deg(p_1), n_1), (\deg(p_2), n_2), \ldots, (\deg(p_k), n_k)).$$

If $\deg(p_i) = 1$ for all i then $(n_1, \ldots, n_k)$ is a shorter notation for type(D).

For example if $D = P_1 + 3P_2$ where P_1 is a place of degree 5 and P_2 a place of degree 1 then

$$type(D) = ((5, 1), (1, 3)).$$

The type of a divisor is stable under the action of $\mathrm{Aut}(C)$.

A.1. **The case $N = 37$ and mdeg > 1.**

A.1.1. *Dominating the set S_2.* Let

$$\texttt{cuspsum} := \sum_{p \in X_1(37)(\mathbb{F}_2)} p$$

(short for rational-cusp-sum) be the sum of all $\mathbb{F}_2$ rational places. Then the set

$$A_2' := \{\texttt{cuspsum} + D \mid D = p_1 + \cdots + p_7 \text{ with } p_1, \ldots, p_7 \in X_1(37)(\mathbb{F}_2)\}$$

dominates S_2. However, A_2' contains many divisors. Using divisors of higher degree, of the form $k \cdot \texttt{cuspsum} + \cdots$ for $k = 1, 2, 3$ depending on type(D), we can dominate S_2 with much fewer divisors. To prove:

$$\min\{\deg(f) \mid f \in H^0(X_1(37)_{\mathbb{F}_2}, \texttt{cuspsum} + D) - \mathbb{F}_2\} \geqslant 18 \tag{4}$$

for all $\texttt{cuspsum} + D$ in A_2' we divide the computation: The table below list for each type(D) (a partition of 7) from which Magma calculation we can conclude inequality (4) for that type.

type(D)	calculation
(7), (6, 1) and (5, 2)	1
(5, 1, 1), (4, 3), (4, 2, 1), (4, 1, 1, 1) and (3, 3, 1)	2
(3, 2, 2)	3
(3, 2, 1, 1) and (3, 1, 1, 1, 1)	2
(2, 2, 2, 1), (2, 2, 1, 1, 1), (2, 1, 1, 1, 1, 1), (1, 1, 1, 1, 1, 1, 1)	4

As in Section 3.2, start the computation by loading the file `X1_37_AFF.m`. Next, load the program `FunctionDegrees` and then run the following:

```
> //calculation 1
> p := plc1[1];
> [Dimension(cuspsum + 6*p + 2*P) : P in plc1];
[ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ]
> //calculation 2
> Min(&cat[FunctionDegrees(2*cuspsum + 4*p + 2*P) : P in plc1]);
18 105
> //calculation 3
> s := Subsets(SequenceToSet(plc1[2..18]),2);
> &cat[FunctionDegrees(cuspsum + 3*p + 2*(&+PQ)) : PQ in s];
[]
> //calculation 4
> Min(FunctionDegrees(3*cuspsum - 4*p);
18 48
```

The set A_2 in the proof of Proposition 3 is the set of divisors occurring in the four calculations above. Calculation 4 used that if $f \in \mathbb{F}_2(X_1(37))$ has $\deg(f) \leqslant 17$ then at least one of $f, f+1$ has an $\mathbb{F}_2$-rational root since $\#X_1(37)(\mathbb{F}_2) = 18$.

A.1.2. *Dominating the set S_3.* The set

$$A_3' := \{\texttt{cuspsum} + D \mid D \geqslant 0,\ \deg(D) = 12 \text{ with } \geqslant 1 \text{ nonrational place}\}$$

dominates all functions in S_3. This time we break up the computation into the following types where we use the following shorthand notation

$$a(c,d) := \underbrace{(c,d),\ldots,(c,d)}_{a}$$

type(D) covered by calculation #c	c
((12,1)) and ((11, 1),(1,1))	1
((10,1),(1,2)) and ((10,1),(1,1),(1,1))	2
((9,1)(1,3))	3
((9,1),(1,2),(1,1)) and ((9,1),(1,1),(1,1),(1,1))	4
((7,1),(1,5)), ((7,1),(1,4),(1,1)) and ((7,1),(1,3),(1,2))	5
((7,1),(1,3),(1,1),(1,1)) and ((7,1),(1,2),(1,2),(1,1))	6
((7,1),(1,2),3(1,1)) and ((7,1),5(1,1))	7
((6,2)) and ((6,1),(6,1))	8
((6,1),(1,6)), ((6,1),(1,5),(1,1)), ((6,1),(1,4),(1,2)), ((6,1),(1,3),(1,3))	9
((6,1),(1,4),2(1,1)), ((6,1),(1,3),(1,2),(1,1)), ((6,1),3(1,2))	10
((6,1),2(1,2),2(1,1)),((6,1),(1,3),3(1,1)),((6,1),(1,2),4(1,1)),((6,1),6(1,1))	11

$X_1(37)_{\mathbb{F}_2}$ has no places of degrees 2–5 and 8. So any non-rational place contributes at least 6 to $\deg(D)$, a fortunate fact that reduces the number of divisors to a

manageable level. The Magma commands to cover these 11 cases are similar to those in Section A.1.1 and can be copied from [DvH].

Theorem 4. *The values in Table 1 are upper bounds for the gonality of $X_1(N)$ over $\mathbb{Q}$. For $N \leqslant 40$ they are exact values.*

Proof. The functions listed at [DvH] are explicit proofs for the upper bounds in Table 1. Section 3, Appendix A, and the accompanying Magma files on [DvH] prove that the bounds are sharp for $N \leqslant 40$. □

References

[Abr96] D. Abramovich. A linear lower bound on the gonality of modular curves. *Internat. Math. Res. Notices*, **20**:1005–1011, 1996.

[BGGP05] M.H. Baker, E. Gonzalez-Jimenez, J. Gonzalez, B. Poonen. Finiteness results for modular curves of genus at least 2. *American J. of Math.*, **127**(6):1325–1387, 2005.

[Der12] M. Derickx. Torsion points on elliptic curves and gonalities of modular curves. Master's thesis, Universiteit Leiden, 2012.

[Deu42] M. Deuring. Reduktion algebraischer funktionenkörper nach primdivisoren des konstantenkörpers. *Mathematische Zeitschrift*, **47**(1):643–654, 1942.

[DvH] M. Derickx and M. van Hoeij. `www.math.fsu.edu/~hoeij/files/X1N` Files: `gonality` (upper bounds with explicit functions g_N, and an overview), `Subfields` (other sources of upper bounds) `cusp_divisors` (divisors of $f_2, f_3, \ldots$), and folder `LowerBoundsGonality` (Magma files for proving lower bounds).

[Fre94] G. Frey. Curves with infinitely many points of fixed degree. *Israel Journal of Mathematics*, **85**(1-3):79–83, 1994.

[JKL11a] D. Joen, C.H. Kim, and Y. Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Mathematics of Computation*, **80**, 579–591, 2011.

[JKL11b] D. Joen, C.H. Kim, and Y. Lee. Families of elliptic curves over quartic number fields with prescribed torsion subgroups. *Mathematics of Computation*, **80**, 2395–2410, 2011.

[K86] S. Kamienny. Torsion points on elliptic curves over all quadratic fields. *Duke Mathematics Journal*, **53**, 157–162, 1986.

[KL81] D. Kubert and S. Lang. *Modular Units (Grundlehren der mathematischen Wissenschaften)*. Springer, 1981.

[Sut12] A.V. Sutherland. Constructing elliptic curves over finite fields with prescribed torsion. *Math. Comp.*, **81**(278):1131–1147, 2012.

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands.

E-mail address: `maarten@mderickx.nl`

Department of Mathematics, Florida State University, Tallahassee, Florida 32306, USA.

Supported by NSF grants 1017880 and 1319547.

E-mail address: `hoeij@math.fsu.edu`