Low Degree Places on the Modular Curve $X_1(N)$

Mark van Hoeij*
Florida State University, Tallahassee, FL 32306-3027, USA
hoeij@math.fsu.edu

February 22, 2012

Let $\alpha := 2\cos(2\pi/7)$ and let τ be the golden ratio, they are solutions of

$$\alpha^3 + \alpha^2 - 2\alpha - 1 = 0, \quad \tau^2 - \tau - 1 = 0.$$

Let

$$b := (6\tau - 3)\alpha^2 + (14\tau - 8)\alpha + 5\tau - 3$$

and

$$c := \tau\alpha^2 + 2\tau\alpha + 1.$$

Let $E_{b,c}$ be the elliptic curve

$$E_{b,c} := y^2 + (1-c)xy - by = x^3 - bx^2 \tag{1}$$

and

$$P := (x = 0, y = 0).$$

Then P is a point on $E_{b,c}$ of order 37. The pair $(E_{b,c}, P)$ corresponds to a point on the modular curve $X_1(37)$. The interest in this example lies in the fact that this point is defined over a number field $\mathbb{Q}(\alpha, \tau)$ of degree 6, whereas the $\mathbb{Q}$-gonality of $X_1(37)$ is 18. This short note is motivated by the following question: Are there only finitely many points on $X_1(N)$ with degree less than the $\mathbb{Q}$-gonality, and if so, can they all be found with a finite computation?

Notations: Let C_N denote the function field of $X_1(N)$ over $\mathbb{Q}$. We can write $C_N = \mathbb{Q}(x)[y]/(F_N)$ where F_N is an explicit equation given by Sutherland at: `http://math.mit.edu/~drew/X1_altcurves.html` The $\mathbb{Q}$-gonality of $X_1(N)$ is

$$\mathrm{gon}(N) := \min\{\mathrm{degree}(f) \mid f \in C_N - \mathbb{Q}\}.$$

Denote Places(N) as the set of discrete valuations on C_N over $\mathbb{Q}$. For each place v, denote $\mathbb{Q}(v)$ as the residue-field of v, and $\deg(v) := [\mathbb{Q}(v) : \mathbb{Q}]$. Consider the

*Supported by NSF grant 1017880.

functions $r, s, b, c \in C_N$ written on Sutherland's webpage as:

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

Then let $j \in C_N$ be the j-invariant of the curve $E_{b,c}$ from equation (1). The *cusps* are the places where $E_{b,c}$ degenerates,

$$\mathrm{Cusps}(N) := \{v \in \mathrm{Places}(N) \,|\, v(j) < 0\}.$$

If v is not a cusp, then v corresponds to an elliptic curve $E_{b,c}$ over $\mathbb{Q}(v)$ with a point P of order N.

In a joint work with Maarten Derickx, $\mathrm{gon}(N)$ has been computed for all $N \leq 40$. The paper is in progress, but the gonality data is available:
`http://www.math.fsu.edu/~hoeij/files/X1N/gonality`
This URL also enumerates all decompositions of $X_1(N) \to X_1(1)$ (i.e. decompositions of the function j). It also lists upper bounds for $\mathrm{gon}(N)$ for $N \leq 100$ (these upper bounds are likely sharp, but that is only proven for $N \leq 40$).

Definition 1. *Define the set of* **low-degree places** *as*

$$\mathrm{LDP}(N) := \{v \in \mathrm{Places}(N) - \mathrm{Cusps}(N) \mid \deg(v) < \mathrm{gon}(N)\}.$$

Let $f \in C_N - \mathbb{Q}$. The support *of f is* $\mathrm{Supp}(f) := \{v \in \mathrm{Places}(N) \,|\, v(f) \neq 0\}$. *We call f a* cusp-function *if* $\mathrm{Supp}(f) \subseteq \mathrm{Cusps}(N)$.
A cusp-neighbor *is a place $v \in \mathrm{Places}(N) - \mathrm{Cusps}(N)$ for which there exists $f \in C_N$ with $v(f) = 1$ and* $\mathrm{Supp}(f) \subseteq \mathrm{Cusps}(N) \bigcup \{v\}$. *We are only interested in low-degree cusp-neighbors, i.e.* $\deg(v) < \mathrm{gon}(N)$.

The example on page 1 shows $\mathrm{LDP}(37) \neq \emptyset$. The main question is: Is $\mathrm{LDP}(N)$ always finite, and can it be computed in a finite number of steps?

For any given N, the set of low-degree cusp-neighbors is finite, and can be computed in a finite number of steps. The question, however, is if this would produce all low-degree places:

Question 1. *Is every low-degree place a cusp-neighbor?*

The author has computed a number of low-degree places by computing Riemann-Roch spaces $L(D)$ for suitably chosen divisors D with $\mathrm{Supp}(D) \subseteq \mathrm{Cusps}(N)$. Combining this with $L(D)$-computations over a finite field[1] the author estimates that it should be possible to find all low-degree cusp-neighbors on a computer for $N \leq 40$. This strategy has not yet been systematically implemented, but the author has tested it to see if it can produce explicit examples, which it does:

[1]To decide which D's to use, consider all divisors D' over $\mathbb{F}_p$ with $D' \geq 0$, $\deg(D') < \mathrm{gon}(N)$, and $\mathrm{Supp}(D') \bigcap \mathrm{Cusps}(N) = \emptyset$. For each such D', compute, if it exists, a D with $\mathrm{Supp}(D) \subseteq \mathrm{Cusps}(N)$ for which $D - D'$ is principal. Lift such D to characteristic 0.

Examples:

The $\mathbb{Q}$-gonality of $X_1(29)$ is 11. A low-degree place of $X_1(29)$ is given below, in the form $(E_{b,c}, P)$, for three non-isomorphic number fields. Additional places over the same fields can be found by taking multiples of P. To decide whether or not $X_1(29)$ has more low-degree places, one needs an answer to Question 1, and, a systematic implementation. The examples can be copied from `www.math.fsu.edu/~hoeij/files/X1N`

Let a be a solution of $a^9 - a^8 - 5a^7 + 5a^6 + 7a^5 - 8a^4 - 2a^3 + 4a^2 - a - 1 = 0$.
$b := a^7 - 5a^6 - 3a^5 + 22a^4 - 3a^3 - 28a^2 + 9a + 8$,
$c := -2a^8 + 2a^7 + 10a^6 - 10a^5 - 16a^4 + 15a^3 + 10a^2 - 6a - 3$.
Then $E_{b,c}$ has a point $P = (0, 0)$ of order $N = 29$.

Let $a^{10} - 2a^7 + a^5 + 2a^4 + 3a^3 - 3a^2 - 2a + 1 = 0$,
$b := (-145a^9 - 14a^8 - 66a^7 + 114a^6 + 175a^5 - 137a^4 - 211a^3 - 324a^2 - 85a + 92)/43$,
$c := a^9 + a^7 - a^6 - a^5 + a^4 + a^3 + 3a^2 + a - 1$.

Let $a^{10} - 2a^9 + 2a^8 - 5a^7 + 7a^6 - 4a^5 + 4a^4 - 8a^3 + 5a^2 - 1 = 0$,
$b := (-23a^9 + 21a^8 + 19a^7 - 71a^6 + 95a^5 - 159a^4 + 178a^3 - 78a^2 - 10a + 6)/97$,
$c := (60a^9 - 59a^8 + 39a^7 - 207a^6 + 98a^5 + 31a^4 + 8a^3 - 58a^2 + 5a - 3)/97$.

The next examples are for $X_1(31)$. Five non-isomorphic fields are given, one of which has degree 9. The $\mathbb{Q}$-gonality of $X_1(31)$ is 12.

Let $a^9 - 3a^8 + 4a^7 - a^6 - 7a^5 + 11a^4 - 9a^3 + 3a^2 - a + 1 = 0$,
$b := (-90a^8 + 228a^7 - 335a^6 + 205a^5 + 183a^4 - 246a^3 + 229a^2 + 49a + 66)/37$,
$c := (-48a^8 + 129a^7 - 117a^6 - 51a^5 + 364a^4 - 368a^3 + 169a^2 - a + 50)/37$.

Let $a^{10} + 2a^8 - 3a^7 + 3a^6 - 7a^5 + 8a^4 - 7a^3 + 7a^2 - 4a + 1 = 0$,
$b := 62a^9 - 48a^8 + 47a^7 - 192a^6 + 262a^5 - 321a^4 + 421a^3 - 330a^2 + 131a - 21$,
$c := 8a^9 + 6a^8 + 4a^7 - 16a^6 + 2a^5 - 8a^4 + 10a^3 + 14a^2 - 16a + 5$.

Let $a^{11} - 2a^{10} - 3a^9 + 9a^8 - a^7 - 13a^6 + 9a^5 + 7a^4 - 5a^3 - 1 = 0$,
$b := -9a^{10} + 38a^9 - 35a^8 - 59a^7 + 131a^6 - 45a^5 - 81a^4 + 59a^3 + 6a^2 + 2a + 14$,
$c := 3a^9 - 7a^8 - 3a^7 + 18a^6 - 9a^5 - 13a^4 + 10a^3 + 9a^2 + 2a$.

Let $a^{11} - 4a^{10} + 9a^9 - 15a^8 + 21a^7 - 21a^6 + 17a^5 - 8a^4 + 3a^2 - 3a + 1 = 0$,
$b := -a^{10} - 3a^9 - 4a^8 - 6a^7 - 6a^6 - a^5 - 6a^4 + 6a^3 - 2a^2 + 3a + 1$,
$c := -a^{10} + 2a^9 - 3a^8 + 3a^7 - 5a^6 - a^5 - a^4 - 3a^3 + 2a^2 - a + 2$.

Let $a^{11} - a^{10} - 4a^9 + 7a^8 + 4a^7 - 9a^6 - 5a^5 + 2a^4 + 8a^3 + 2a^2 - 3a - 1 = 0$,
$b := (-245a^{10} + 1414a^9 + 3377a^8 - 3908a^7 - 7202a^6 + 562a^5 + 5683a^4 + 5190a^3 - 449a^2 - 2406a - 678)/349$, $c := (8a^{10} - 106a^9 - 304a^8 + 290a^7 + 842a^6 - 440a^5 - 932a^4 + 265a^3 + 395a^2 - 24a - 79)/349$.

We end with one more question (note: this holds for $N \leq 40$):

Question 2. *Must C_N have a cusp-function of degree* $\mathrm{gon}(N)$*?*

The author would like to thank Maarten Derickx and Andrew Sutherland for fruitful discussions.