JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **28**, No. 3, August 2015
http://dx.doi.org/10.14403/jcms.2015.28.3.443

POINTS ON MODULAR CURVES OVER FINITE FIELDS

Daeyeol Jeon*

Abstract. In this paper we propose a method of computing the number of points on the reduction of non-hyperelliptic modular curves of genus greater than or equal to 3 over finite fields.

1. Introduction

Let N be a positive integer, and let

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,|\, c \equiv 0 \mod N \right\}.$$

Let $X_0(N)$ denote the modular curve corresponding to $\Gamma_0(N)$ and $g_0(N)$ denote its genus. The modular curve $X_0(N)$(with cusps removed) para metrizes isomorphism classes of pairs (E, C), where E is an elliptic curve and C is a cyclic subgroup of E of order N.

A curve X defined over an algebraically closed field k is called *d-gonal* if it admits a map $\phi : X \to \mathbb{P}^1$ over k of degree d. The smallest possible d is called the *gonality* of X denoted by $\mathrm{Gon}(X)$. If a curve X is 2-gonal and its genus $g(X) \geq 2$, then X is said to be *hyperelliptic*. If a curve X is 3-gonal, then we call X *trigonal*.

Ogg [4] determined all values of N for which $X_0(N)$ is hyperelliptic, and Hasegawa and Shimura [2] determined all the trigonal curves $X_0(N)$. A crucial instrument used in their proofs is $\#\tilde{X}_0(N)(\mathbb{F}_{p^2})$ which denote the number of points on the reduction of $X_0(N)$ over the finite fields $\mathbb{F}_{p^2}$ where p is a prime with $p \nmid N$. Note that for a prime $p \nmid N$, the

Received May 08, 2015; Accepted July 31, 2015.
2010 Mathematics Subject Classification: Primary 11G05; Secondary 11G18.
Key words and phrases: modular curve, finite field.
This research was supported by the research year project of the Kongju National University in 2014 and by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2014R1A1A2056390).

curve $X_0(N)$ has good reduction. Indeed Ogg [4] proposed a method to give a lower bound for $\#\tilde{X}_0(N)(\mathbb{F}_{p^2})$ by computing the pairs (E, C) with supersingular elliptic curves E and their cyclic subgroups C of order N.

In this paper, we propose a method of computing the exact number of points on the reduction of non-hyperelliptic modular curves $X_0(N)$ of $g_0(N) \geq 3$ over any finite fields whose characteristic does not divide N. This method can be applied for another sort of modular curves defined over $\mathbb{Q}$.

Indeed, such a method is well-known for rational, elliptic or hyperelliptic modular curves.

2. Preliminaries

Suppose $X_0(N)$ is a non-hyperelliptic modular curve of $g := g_0(N) \geq 3$. In this section, we consider a method to find the canonical embedding of $X_0(N)$ which is described in [2, 3]. The canonical embedding of $X_0(N)$ is the embedding

$$X_0(N) \ni P \mapsto [\omega_1(P) : \cdots : \omega_g(P)] \in \mathbb{P}^{g-1}$$

determined by the canonical linear system. Its image is called a *canonical curve*.

The space $\Omega^1(X_0(N))$ of holomorphic differentials is isomorphic to the space of weight 2 cusp forms, $S_2(N)$, on $X_0(N)$. Indeed, let $\{f_1, \ldots, f_g\}$ be a basis for $S_2(N)$, then the set $\{f_i(\tau)d\tau\}$ forms a basis for $\Omega^1(X_0(N))$. Then the canonical embedding of $X_0(N)$ is given by

$$X_0(N) \ni P \mapsto [f_1(P) : \cdots : f_g(P)] \in \mathbb{P}^{g-1}.$$

This image is a curve of degree $2g - 2$ and it will be described by some set of projective equations of the form $F(f_1, \ldots, f_g) = 0$. We call these equations a *canonical model* of $X_0(N)$.

To construct a canonical model we take the q-expansions of a basis for the space $S_2(N)$ which can be computed by using a computer algebra system SAGE. Here $q = e^{2\pi i\tau}$ and τ is in the complex upper half plane. Then we compute a canonical model by finding combinations of powers of the q-expansions which yield identically zero series. We know that for almost all N canonical models consist of polynomials of degree 2 from the following result.

THEOREM 2.1. [1, 5] *Let X be a canonical curve of genus ≥ 4 defined over an algebraically closed field. Then the ideal $I(X)$ of X is generated by some quadratic polynomials, unless X is trigonal or isomorphic to* *a smooth plane quintic curve, in which cases it is generated by some quadratic and (at least one) cubic polynomials.*

For the reader's convenience, we make lists of N for which $X_0(N)$ is rational, elliptic, hyperelliptic or of that $\mathrm{Gon}(X_0(N)) = 3$.

THEOREM 2.2. [2, 4] *The following holds:*

(a) $X_0(N)$ *is rational only for* N*:* $1-10$, 12, 13, 16, 18, 25.
(b) $X_0(N)$ *is elliptic only for* N*:* 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49.
(c) $X_0(N)$ *is hyperelliptic only for* N*:* 22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71.
(d) $\mathrm{Gon}(X_0(N)) = 3$ *only for* N*:* 34, 38, 43, 44, 45, 53, 54, 61, 64, 81.

3. Canonical models

In this section, we explain how to compute a canonical model of $X_0(N)$. Consider $X_0(42)$ of genus 5. In SAGE one can compute q-expansions of a basis for $S_2(42)$ by using the following commands:

```
M = ModularForms(Gamma0(42));
S = M.cuspidal_submodule();
S.q_expansion_basis(100);
```

Then we have the following:

$$
\begin{aligned}
f_1 =& q + q^6 + q^7 - 2q^8 - 3q^9 - 2q^{10} - q^{12} - \cdots ,\\
f_2 =& q^2 - q^8 - q^9 - 2q^{10} - 2q^{11} + 2q^{13} - \cdots ,\\
f_3 =& q^3 - q^6 - 2q^9 + q^{12} + 2q^{18} + q^{21} - \cdots ,\\
f_4 =& q^4 - q^6 - q^9 - 2q^{11} + q^{12} + 2q^{13} + \cdots ,\\
f_5 =& q^5 + q^6 + q^7 - 2q^8 - 2q^9 - q^{10} - \cdots .
\end{aligned}
$$

By Theorem 2.1, the defining ideal of the canonical curve in $\mathbb{P}^4$ of $X_0(42)$ generated by quadratic polynomials, and hence it suffices to consider the relations of $\frac{g(g+1)}{2} = 15$ monomials $\{f_i f_j\}$ with $1 \le i \le j \le 5$ for getting a canonical model of $X_0(42)$.

Put $A = (a_{mn})$ the 99×15 matrix with a_{mn} being the coefficient of q^m in the q-expansion of the n-th element $f_k f_l$ of $\{f_i f_j\}$.

N	Canonical model of $X_0(N)$
34	$x^4 + x^3z - 2x^2z^2 + 3xy^2z + xz^3 - y^4 + z^4$
38	$-y^2 + zx - z^2 - wy - wz - w^2$, $y^2x - 3y^3 - zx^2 + 4zyx - 3zy^2 + z^2x - z^2y - z^3$ $-wx^2 + wyx - 4wy^2 - wzx + w^3$
42	$-y^2 + zx + vz$, $-zy - z^2 + vx + vy + vz - v^2 + wz - 2wv$, $z^2 - wx + wy - wv + w^2$
43	$x^4 + 2x^3y + 2x^2y^2 + 2x^2yz + 4x^2z^2$ $+xy^3 + 2xy^2z + 4xyz^2 + y^3z + 2y^2z^2 + 3yz^3 + 4z^4$
44	$-x^2 - 4yx - 8y^2 - 4zx - 16zy - 16z^2 + w^2$, $-y^3 + zx^2 + 4zyx + 4z^2x$
45	$x^4 + 2x^3y + x^2y^2 + x^2yz - x^2z^2 - xy^2z + 3xyz^2$ $-2xz^3 - y^3z + y^2z^2 + yz^3 + 4z^4$

Table 1. Canonical models for $X_0(N)$

Solving the linear equation $AX = 0$ with $X = \begin{pmatrix} x_1 \\ \vdots \\ x_{15} \end{pmatrix}$, we can find three relations between $\{f_i f_j\}$, and they give a canonical model of $X_0(42)$ as follows:

$$
\begin{aligned}
F_1 :&\ \ -y^2 + zx + vz, \\
F_2 :&\ \ -zy - z^2 + vx + vy + vz - v^2 + wz - 2wv, \\
F_3 :&\ \ z^2 - wx + wy - wv + w^2,
\end{aligned} \tag{3.1}
$$

where the variables x, y, z, v, w are corresponding to f_1, f_2, f_3, f_4, f_5, respectively.

We omit an explanation for the canonical curves whose defining ideals contain a cubic polynomial for which one can refer [2, 3].

We list canonical models for $X_0(N)$ in Table 1 where $X_0(N)$ is a non-hyperelliptic curve of genus greater than or equal to 3 for $N \leq 50$. We note that the canonical models for $X_0(N)$ with $N = 34, 43, 45$ are directly from Table 1 in [3]. Indeed, such curves are of genus 3 and defined by plane quartic polynomials.

4. Points on modular curves over a finite field

Suppose $X_0(N)$ is a non-hyperelliptic modular curve of genus $g \geq 3$. Now we explain how to compute $\#\tilde{X}_0(N)(\mathbb{F}_q)$ where $q = p^k$ and $p \nmid N$. Suppose $\{F_1, F_2, \dots, F_n\}$ is a canonical model of $X_0(N)$ with integer coefficients. Put $G_i := F_i \mod p$ for $i = 1, 2, \dots, n$. Let Y be the curve defined by $\{G_1, G_2, \dots, G_n\}$ over $\mathbb{F}_p$. Our basic strategy is to compute the number of $\mathbb{F}_q$-rational points $\#Y(\mathbb{F}_q)$ on Y. However we don't know whether it defines a non-singular curve. In fact, Galbraith [3] appointed that the canonical model of $X_0(38)$ he obtained first has bad reduction at the prime 3 even though 38 is not divisible by 3. By a proper change of coordinates, he could obtain a canonical model for $X_0(38)$ which has good reduction at 3. We note that the canonical model for $X_0(44)$ in Table 1 is not computed by the basis of $S_2(44)$ obtained from Singular but the basis $\{f(\tau), f(2\tau), f(4\tau), g(\tau)\}$ where $f(z)$(resp. $g(\tau)$) is the normalized eigenform of Hecke operators in $S_2(11)$(resp. $S_2(44)$). The canonical model for $X_0(44)$ obtained by using the basis of $S_2(44)$ from Singular has bad reduction at 3.

A computer algebra system Macaulay2 enables us to determine whether the reduction of a canonical model of $X_0(N)$ has good reduction over $\mathbb{F}_q$.

First, we compute the arithmetic genus of Y which should be equal to the (geometric) genus of $X_0(N)$. It can be computed by the following comments:

```
R=ZZ/p[x_1,x_2,...,x_g]
I=ideal{G_1,j,G_2,...,G_n}
genus(I)
```

Second, we check Y has no singularities over $\mathbb{F}_q$ by the following comments:

```
R=GF(q)[x_1,x_2,...,x_g]
I=ideal{G_1,j,G_2,...,G_n}
sing=singularLocus(R/I)
codim(sing)
```

If it gives the co-dimension g of singular locus, then we can conclude that Y has no singularity over $\mathbb{F}_q$. However, we are not sure that Y has no singularities over the algebraic closure $\bar{F}_p$. Nevertheless it suffices to compute $\#Y(\mathbb{F}_q)$ for obtaining $\#\tilde{X}_0(N)(\mathbb{F}_q)$.

N	p	$\#\tilde{X}_0(N)(\mathbb{F}_p)$	$\#\tilde{X}_0(N)(\mathbb{F}_{p^2})$
34	3	6	24
38	3	8	24
42	5	12	64
43	2	5	9
44	3	6	30
45	2	4	14

TABLE 2. Number of points $\#\tilde{X}_0(N)(\mathbb{F}_q)$

THEOREM 4.1. *Suppose $X_0(N)$ is a non-hyperelliptic curve of genus $g \geq 3$, and its canonical model $\{F_1, F_2, \ldots, F_n\}$ consists of polynomials with integer coefficients. Let Y be a curve defined by $\{G_1, G_2, \ldots, G_n\}$ over $\mathbb{F}_p$ where $G_i := F_i \mod p$ with $p \nmid N$. Suppose Y has geometric genus g and no singularities over $\mathbb{F}_q$ with $q = p^k$, then $\#Y(\mathbb{F}_q)$ is the same as $\#\tilde{X}_0(N)(\mathbb{F}_q)$.*

Proof. If Y is a non-singular curve, then the result is true. Suppose Y has singular points $P_1, \ldots, P_m$ over a finite extension $\mathbb{F}_r$ of $\mathbb{F}_q$. For getting a smooth model for Y we need to blow Y up. Since the set $\{P_1, \ldots, P_m\}$ is Galois invariant, the blown up curve Z will be defined over $\mathbb{F}_q$. And the blow-down map $\pi : Z \to Y$ is defined over $\mathbb{F}_q$ too. It follows that the fields of definition of points in $\pi^{-1}(P_i)$ must contain the field of definition of P_i, hence are not equal to $\mathbb{F}_q$. This proves that π is a bijection on the $\mathbb{F}_q$-rational points, i.e. $\pi : Z(\mathbb{F}_q) \to Y(\mathbb{F}_q)$ is an isomorphism. By definition, $\#\tilde{X}_0(N)(\mathbb{F}_q)$ is $\#Z(\mathbb{F}_q)$, so the result is true. $\square$

EXAMPLE 4.2. *Let Y denote the curve over $\mathbb{F}_5$ defined by the reduction $\{G_1, G_2, G_3\}$ modulo 5 of a canonical model of $X_0(42)$ described in (3.1). Using Macaulay2 we can check that Y has arithmetic genus 5 and no singularities over $\mathbb{F}_{25}$. Plugging in all values of x, y, z, v, w and counting those for which $G_1 \equiv G_2 \equiv G_3 \equiv 0 \pmod 5$, we can get $\#\tilde{X}_0(42)(\mathbb{F}_5) = 12$ and $\#\tilde{X}_0(42)(\mathbb{F}_{25}) = 64$.*

By using the method suggested in this paper, we compute $\#\tilde{X}_0(N)(\mathbb{F}_p)$ and $\#\tilde{X}_0(N)(\mathbb{F}_{p^2})$ in Table 2 where $X_0(N)$ is a non-hyperelliptic curve of $g_0(N) \geq 3$ for $N \leq 50$ and p is the smallest prime $p \nmid N$.

Acknowledgments

This paper was written during my sabbatical leave at Brown University. We thank Joseph Silverman for his comments in proving Theorem 4.1, and we thank Jeaman Ahn for the comments for Macaulay2. We are grateful to department of mathematics of Brown university for their support and hospitality.

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of Algebraic Curves,* Vol. I, Grundlehren Math. Wiss. **267**, Springer-Verlag, New York, 1985.

[2] Y. Hasegawa and M. Shimura, *Trigonal modular curves,* Acta Arith., **88** (1999), 129–140.

[3] S. D. Galbraith, *Equations for modular curves,* Ph. D. Thesis, University of Oxford (1996).

[4] A. Ogg, *Hyperelliptic modular curves,* Bull. Soc. Math. France **102** (1974), 449-462.

[5] B. Saint-Donat, *On Petri's analysis of the linear system of quadrics through a canonical curve*, Math. Ann. **206** (1973), 157-175.

*
Department of Mathematics education
Kongju National University
Gongju 314-701, Republic of Korea
E-mail: dyjeon@kongju.ac.kr