axioms

Article

The Recursive Structures of Manin Symbols over $\mathbb{Q}$, Cusps and Elliptic Points on $X_0(N)$

Sanmin Wang

Faculty of Science, Zhejiang Sci-Tech University, Hangzhou 310018, China; wangsanmin@zstu.edu.cn

Abstract: Firstly, we present a more explicit formulation of the complete system $D(N)$ of representatives of Manin's symbols over $\mathbb{Q}$, which was initially given by Shimura. Then, we establish a bijection between $D(M) \times D(N)$ and $D(MN)$ for $(M,N) = 1$, which reveals a recursive structure between Manin's symbols of different levels. Based on Manin's complete system $\Pi(N)$ of representatives of cusps on $X_0(N)$ and Cremona's characterization of the equivalence between cusps, we establish a bijection between a subset $C(N)$ of $D(N)$ and $\Pi(N)$, and then establish a bijection between $C(M) \times C(N)$ and $C(MN)$ for $(M,N) = 1$. We also provide a recursive structure for elliptical points on $X_0(N)$. Based on these recursive structures, we obtain recursive algorithms for constructing Manin symbols over $\mathbb{Q}$, cusps, and elliptical points on $X_0(N)$. This may give rise to more efficient algorithms for modular elliptic curves. As direct corollaries of these recursive structures, we present a recursive version of the genus formula and prove constructively formulas of the numbers of $D(N)$, cusps, and elliptic points on $X_0(N)$.

Keywords: modular curve; elliptic curve; recursive structure; Manin's symbols over $\mathbb{Q}$; cusps; elliptic points; algorithmic number theory

MSC: 11A05; 11F06; 20H05; 20J05

check for updates

Citation: Wang, S. The Recursive Structures of Manin Symbols over $\mathbb{Q}$, Cusps and Elliptic Points on $X_0(N)$. *Axioms* **2023**, *12*, 597. https://doi.org/10.3390/axioms12060597

Academic Editors: Emil Saucan and David Xianfeng Gu

Received: 13 May 2023
Revised: 12 June 2023
Accepted: 14 June 2023
Published: 16 June 2023

1. Introduction

In his seminal monograph [1] (Chapter 1, Proposition 1.43), G. Shimura defined a complete set $D(N)$ of representatives for the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ over $\mathbb{Z}/N\mathbb{Z}$ to be all couples $\{c,d\}$ of positive integers satisfying

$$(*)\ (c,d) = 1, d|N, 1 \leqslant c \leqslant N/d (or\ c\ in\ any\ set\ of\ representatives\ for\ \mathbb{Z}\ modulo\ (N/d)),$$

where (c,d) denote the greatest common divisor of integers c and d.

Let $[x]$ be the greatest integer less than or equal to x. For two integers a,b with $b \neq 0$, define

$$[\frac{a}{b}]' = \begin{cases} \frac{a}{b} - 1 & \text{if } b|a, \\ [\frac{a}{b}] & \text{otherwise,} \end{cases}$$

then $1 \leqslant a - b[\frac{a}{b}]' \leqslant b$. In this paper, we define

$$\begin{aligned} D(N) = \{(c,d) : c,d \in \mathbb{Z}, c,d \geqslant 1, c|N, (c,d) = 1\ and \\ (c, d - \frac{N}{c}([\frac{cd}{N}]' - n)) \geqslant 2\ for\ 0 \leqslant n < [\frac{cd}{N}]'\}. \end{aligned} \tag{1}$$

We then establish a bijection between $D(M) \times D(N)$ and $D(MN)$ for $(M,N) = 1$ in Section 2. This result gives a recursive algorithm to construct the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ over $\mathbb{Z}/N\mathbb{Z}$.

Let $\Pi(N) = \{[\delta;\ a \bmod (\delta, N\delta^{-1})] : a, \delta \in \mathbb{Z}, \delta \geqslant 1, \delta|N, 1 \leqslant a \leqslant (\delta, N\delta^{-1})\}$. In [2] (Proposition 2.2), Manin proved that there exists a bijection between $\Pi(N)$ and the set of cusps on $X_0(N)$. Based on Manin's result and Cremona's characterization (See Proposition 3), we identify $\Pi(N)$ with

$$\begin{aligned} C(N) = \{(c,d) : c,d \in \mathbb{Z}, 1 \leqslant c \leqslant N, c|N, (c,d) = 1 \quad \text{and} \\ (c, d - (c, Nc^{-1})[\frac{d}{(c,Nc^{-1})}]' + \frac{Nn}{c}) \geqslant 2 \text{ for } 0 \leqslant n < \frac{c(c,Nc^{-1})}{N}[\frac{d}{(c,Nc^{-1})}]'\}, \end{aligned} \tag{2}$$

which is a subset of $D(N)$. In Section 3, we establish a bijection between $C(N_1N_2)$ and $C(N_1) \times C(N_2)$ for $(N_1, N_2) = 1$. This result gives a recursive algorithm to construct the complete set of representatives of $\Gamma_0(N)$-inequivalent cusps.

Define

$$\begin{aligned} E_2(N) &= \{(1,d) : (1,d) \in D(N), 1 + d^2 \equiv 0 \pmod N\}, \\ E_3(N) &= \{(1,d) : (1,d) \in D(N), 1 - d + d^2 \equiv 0 \pmod N\}. \end{aligned} \tag{3}$$

Then, there exist bijections between $E_2(N), E_3(N)$ and complete sets of representatives of $\Gamma_0(N)$-inequivalent elliptic points of order 2 and 3, respectively. In Section 4, we establish bijections between $E_2(N_1N_2)$ and $E_2(N_1) \times E_2(N_2)$, $E_3(N_1N_2)$ and $E_3(N_1) \times E_3(N_2)$, for $(N_1, N_2) = 1$. These results give a recursive algorithm for constructing the complete set $E_3(N)$ and $E_2(N)$of $\Gamma_0(N)$-inequivalent elliptic points of order 2, 3.

The elements in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ are called Manin symbols [3] (Section 2.2) and there exists a bijection between the set of right cosets of $\Gamma_0(N)$ in $\mathrm{SL}(2,\mathbb{Z})$ and $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ [2] (Proposition 2.4). An important step in the modular elliptic algorithm is to construct a complete set of representatives for the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ and a complete set of representatives of $\Gamma_0(N)$-inequivalent cusps [3] (Chapter II). The recursive structure of $D(N), C(N), E_2(N)$ and $E_3(N)$ may give rise to a more efficient modular elliptic algorithm.

As direct corollaries of these recursive structures, we present a recursive version of the genus formula and elementary proofs of formulas of the numbers $\mu(N)$, $v_\infty(N)$, $v_2(N)$ and $v_3(N)$ of $D(N)$, $C(N)$, $E_2(N)$, $E_3(N)$. Note that Schoeneberg's proof and Shimura's proof for formulas of $\mu(N)$, $v_\infty(N)$, $v_2(N)$ and $v_3(N)$ use the theory of quadratic fields, see [4] (Chapter IV, Section 8) and [1] (Chapter 1, Proposition 1.43). Their proofs may make these formulas hard to approach when compared with our proofs.

2. The Recursive Structure of Manin Symbols over $\mathbb{Q}$

We firstly give some necessary notations and facts, for details, see [3].

Definition 1.

(a) $D_2(N) = \{(c,d) : c,d \in \mathbb{Z}, (c,d,N) = 1\}$;

(b) $\forall (c_1,d_1), (c_2,d_2) \in D_2(N)$, *define* $(c_1,d_1) \sim (c_2,d_2)$ *if* $c_1d_2 \equiv d_1c_2 \pmod N$, *then* $\sim$ *is an equivalence relation on* $D_2(N)$;

(c) $\forall (c,d) \in D_2(N)$, *define* $(c:d) = \{(c',d') : (c',d') \in D_2(N), (c',d') \sim (c,d)\}$;

(d) $\mathcal{D}(N) = D_2(N)/\sim = \{(c:d) : (c,d) \in D_0(N)\}$;

(e) $D_1(N) = \{(c,d) : c,d \in \mathbb{Z}, c,d \geqslant 1, c|N, (c,d,\frac{N}{c}) = 1, cd \leqslant N\}$;

(f) $D(N)$ *is defined in (1);*

(g) $\mu(N)$, $v_\infty(N)$, $v_2(N)$ *and* $v_3(N)$ *are the numbers of elements in* $D(N), C(N), E_2(N)$ *and* $E_3(N)$, *respectively.*

As pointed out by a referee, the index $\mu(N)$ of $\Gamma_0(N)$ in $\mathrm{SL}(2,\mathbb{Z})$ is called the Dedekind psi function, usually denoted $\psi(N)$, see [5,6]. Here, we follow Shimura's notations in [1] (Proposition 1.43).

Lemma 1. *Let $c,d,h \in \mathbb{Z}$, $(c,d,h) = 1, c,d \geqslant 1$ and $d \leqslant h$, then there exists an integer k such that $(c, d+hk) = 1$ and $0 \leqslant k < c$.*

Proof. If $c = 1$, take $k = 0$ then $(c, d+hk) = 1$. Thus, let $c \geqslant 2$ in the following. Let $c = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the standard factorization of c. The proof is by induction on the numbers of distinct prime divisors in c. Suppose that $c = p_1^{\alpha_1}$. Assume that $(p_1^{\alpha_1}, d) \geqslant 2$ and $(p_1^{\alpha_1}, d+h) \geqslant 2$ then $p_1|d$ and $p_1|(d+h)$. Thus, $p_1|d$ and $p_1|h$, this contradicts with $(c,d,h) = 1$, and hence $(c, d+hk) = 1$ for some $0 \leqslant k \leqslant 1 < c$.

Let $c_1 = p_1^{\alpha_1} \cdots p_{s-1}^{\alpha_{s-1}}$. By the induction hypothesis, there exists an integer k_1 such that $(c_1, d+hk_1) = 1$ and $0 \leqslant k_1 < c_1$. Then, $(c_1, d+hk_1+hc_1) = 1$. Assume that $(p_s^{\alpha_s}, d+hk_1) \geqslant 2$ and $(p_s^{\alpha_s}, d+hk_1+hc_1) \geqslant 2$ then $p_s|(d+hk_1)$ and $p_s|(d+hk_1+hc_1)$. Thus, $p_s|hc_1$ and hence $p_s|h$ by $(p_s, c_1) = 1$. Therefore, $p_s|d$. This contradicts with $(c,d,h) = 1$ and hence $(c, d+hk_1) = 1$ or $(c, d+hk_1+hc_1) = 1$. Take $k = k_1$ or$k = c_1 + k_1$, then $(c, d+hk) = 1$ for some $0 \leqslant k_1 \leqslant k \leqslant c_1 + k_1 < 2c_1 \leqslant c$. This completes the proof by the induction principle. □

Corollary 1. *Let $a,b,c \in \mathbb{Z}$, $(a,b,c) = 1$, then the equation $ax+by+cyz = 1$ has solutions in $\mathbb{Z}$.*

Lemma 2. *There exists a bijection between $D(N)$ and $D_1(N)$.*

Proof. Let $(c,d) \in D(N)$. Define $d_n = d - \frac{N}{c}[\frac{cd}{N}]' + \frac{Nn}{c}$ for all $n \in \mathbb{Z}$. Then, $1 \leqslant d_0 \leqslant \frac{N}{c}$ and $(c, d_0, \frac{N}{c}) = 1$ by $(c,d) = 1$. Thus $(c, d_0) \in D_1(N)$. Define $\Phi : D(N) \to D_1(N)$ by sending (c,d) to (c, d_0).

Let $(u,v) \in D(N)$ such that $\Phi(c,d) = \Phi(u,v)$. Define $v_n = v - \frac{N}{u}[\frac{uv}{N}]' + \frac{Nn}{u}$ for all $n \in \mathbb{Z}$. Then, $c = u$ and $d_0 = v_0$. Thus, $d_n = v_n$ for all $n \in \mathbb{Z}$. Let $e = [\frac{cd}{N}]'$ and $w = [\frac{cv}{N}]'$. Then, $d = d_e$ and $v = v_w$. Suppose that $e < w$ then $(c, d_e) = 1$ by $(c,d) = 1$ but $(c, d_e) \geqslant 2$ by $(c,v) \in D(N)$ and $d_e = v_e$, a contradiction and thus $e \geqslant w$. $e \leqslant w$ holds by a similar proof and thus $e = w$ and $(c,d) = (u,v)$. Therefore, Φ is an injection from $D(N)$ to $D_1(N)$.

Let $(c, d_0) \in D_1(N)$. By Lemma 1, there exists an integer k such that $(c, d_0 + \frac{Nk}{c}) = 1$ and $0 \leqslant k \leqslant c-1$. Let $0 \leqslant k_0 \leqslant k$ such that $(c, d_0 + \frac{Nk_0}{c}) = 1$ and $(c, d_0 + \frac{Nn}{c}) = 1$ for all $0 \leqslant n < k_0$. Define $d = d_0 + \frac{Nk_0}{c}$. Then, $(c,d) \in D(N)$ and $\Phi((c,d)) = (c, d_0)$. Therefore, Φ is a surjection from $D(N)$ to $D_1(N)$. □

Lemma 3. *There exists a bijection between $\mathcal{D}(N)$ and $D(N)$, i.e., $D(N)$ is a complete system of the representatives of elements of $\mathcal{D}(N)$.*

Proof. Define $\Phi : D(N) \to \mathcal{D}(N)$ by the natural map, i.e., $\Phi((c,d)) = (c:d)$.

Let $(c:d) \in \mathcal{D}(N)$. Then, $(c,d,N) = 1$. Define $c_1 = (c,N)$, d_0 to be the unique solution of the congruence equation $\frac{c}{c_1}x \equiv d (\bmod\ \frac{N}{c_1})$ such that $1 \leqslant d_0 \leqslant \frac{N}{c_1}$. Then, there exists an integer y such that $\frac{c}{c_1}d_0 + \frac{N}{c_1}y = d$. Assume that there exists a prime p such that $p|(c_1, d_0, \frac{N}{c_1})$. Then, $p|d$ and $p|(c, N)$, this contradicts with $(c, d, N) = 1$, and thus $(c_1, d_0, \frac{N}{c_1}) = 1$. Hence, $(c_1, d_0) \in D_1(N)$. Then, there exists the unique $(c_1, d_1) \in D(N)$ which corresponds to (c_1, d_0). Hence, $(c_1, d_1) \in (c : d)$, i.e., $\Phi((c_1, d_1)) = (c : d)$.

Assume that$(c_1, d_1), (c_2, d_2) \in D(N)$ such that $\Phi((c_1, d_1)) = \Phi((c_2, d_2))$. Then, $(c_1 : d_1) = (c_2 : d_2)$ and thus there exists an integer$k$ such that $c_1 d_2 - c_2 d_1 = Nk$. Thus, $c_1 | c_2 d_1$ by $c_1 | N$ and $c_2 | c_1 d_2$ by $c_2 | N$. Hence, $c_1 | c_2$ by $(c_1, d_1) = 1$ and $c_2 | c_1$ by $(c_2, d_2) = 1$. Therefore, $c_1 = c_2$ and $d_1 = d_2$ by $d_1 \equiv d_2 (\bmod \frac{N}{c_1})$ and the definition of $D(N)$. Thus, Φ is a bijection between $\mathcal{D}(N)$ and $D(N)$. This completes the proof. $\square$

Theorem 1. *Let $M, N \in \mathbb{Z}, M, N \geqslant 1$, $(M, N) = 1$. Then, there exists a bijection between $D(M) \times D(N)$ and $D(MN)$.*

Proof. Let $(a, b) \in D(M)$ and $(c, d) \in D(N)$. Assume that there exists a prime p such that $p|(ac,\ bN + dM - \frac{MN}{ac}[\frac{ac(bN + dM)}{MN}]', \frac{MN}{ac})$. Then, $p|ac, p|\frac{M}{a}\frac{N}{c}$ and

$$p|bN + dM - \frac{MN}{ac}[\frac{ac(bN + dM)}{MN}]'.$$

Then $p|a, p|\frac{M}{a}$ or $p|c, p|\frac{N}{c}$ by $(M, N) = 1$,$a|M, c|N$. If $p|a, p|\frac{M}{a}$ then $p|bN$ and thus $p|N$ by $(a, b) = 1$, which contradicts with $(M, N) = 1$. The case of $p|c, p|\frac{N}{c}$ is tackled in a similar way. Therefore $(ac,\ bN + dM - \frac{MN}{ac}[\frac{ac(bN + dM)}{MN}]', \frac{MN}{ac}) = 1$ and

$$(ac,\ bN + dM - \frac{MN}{ac}[\frac{ac(bN + dM)}{MN}]') \in D_1(MN).$$

Define $e = ac, f = bN + dM - \frac{MN}{ac}([\frac{ac(bN + dM)}{MN}]' - k)$ for some k such that

$$(ac,\ bN + dM - \frac{MN}{ac}([\frac{ac(bN + dM)}{MN}]' - n)) \geqslant 2$$

for all $0 \leqslant n < k$. Then $(e, f) \in D(MN)$. Define $\Phi : D(M) \times D(N) \to D(MN)$ by sending $((a, b), (c, d))$ to (e, f).

Assume that $\Phi((a, b), (c, d)) = \Phi((a_1, b_1), (c_1, d_1))$ for some $(a, b), (a_1, b_1) \in D(M)$ and $(c, d), (c_1, d_1) \in D(N)$. Then

$$(ac,\ bN + dM - \frac{MN}{ac}([\frac{ac(bN + dM)}{MN}]' - k))$$

$$= (a_1 c_1,\ b_1 N + d_1 M - \frac{MN}{a_1 c_1}([\frac{a_1 c_1 (b_1 N + d_1 M)}{MN}]' - k_1)).$$

Thus, $ac = a_1 c_1$ and

$$bN + dM - \frac{MN}{ac}([\frac{ac(bN + dM)}{MN}]' - k)$$

$$= b_1 N + d_1 M - \frac{MN}{a_1 c_1}([\frac{a_1 c_1 (b_1 N + d_1 M)}{MN}]' - k_1).$$

Hence, $a = a_1$, $c = c_1$ by $(M, N) = 1$,$a|M, a_1|M, c|N, c_1|N$. Therefore,

$$bN + dM - \frac{MN}{ac}([\frac{ac(bN + dM)}{MN}]' - k)$$

$$= b_1N + d_1M - \frac{MN}{ac}([\frac{ac(b_1N + d_1M)}{MN}]' - k_1).$$

Thus $d \equiv d_1(\bmod\ \frac{N}{c})$ and $b \equiv b_1(\bmod\ \frac{M}{a})$by $(M, N) = 1$. Hence $b = b_1$, $d = d_1$. Then $((a, b),(c, d)) = ((a_1, b_1),(c_1, d_1))$.

Let $(e, f) \in D(MN)$. Then $e|MN$, $(e, f) = 1$ and $(e, f - \frac{MN}{e}([\frac{ef}{MN}]' - n)) \geqslant 2$ for $0 \leqslant n < [\frac{ef}{MN}]'$. Let $a = (e, M)$, $c = (e, N)$, then $e = ac$, $a|M$ and $c|N$. Let x_0, y_0, z_0 be a particular solution of the equation

$$Nx + My + \frac{MN}{ac}z = f \tag{4}$$

then $x = \frac{M}{a}X + x_0, y = \frac{N}{c}Y + y_0, z = -cX - aY + z_0$ are solutions of (4) for all integers X, Y. Take $b_1 = x_0 - \frac{M}{a}[\frac{ax_0}{M}]', d_1 = y_0 - \frac{N}{c}[\frac{cy_0}{N}]'$, then

$$Nb_1 + Md_1 + \frac{MN}{ac}(c[\frac{ax_0}{M}]' + a[\frac{cy_0}{N}]' + z_0) = f, 1 \leqslant b_1 \leqslant \frac{M}{a}, 1 \leqslant d_1 \leqslant \frac{N}{c}.$$

Then, $(a, b_1, \frac{M}{a}) = 1$ by $a|M,(e, f) = 1$ and $(c, d_1, \frac{N}{c}) = 1$ by $c|N,(e, f) = 1$. Hence, $(a, b_1) \in D_1(M),(c, d_1) \in D_1(N)$. Let $(a, b) \in D(M)$ and $(c, d) \in D(N)$ which correspond to (a, b_1) and (c, d_1), respectively. Then $b = b_1 + \frac{M}{a}k_1$ and $d = d_1 + \frac{N}{c}k_2$ for some k_1, k_2. Then $Nb + Md + \frac{MN}{ac}(c[\frac{ax_0}{M}]' + a[\frac{cy_0}{N}]' - ck_1 - ak_2 + z_0) = f$. Then $(e, f) = \Phi((a, b),(c, d))$.

Thus, Φ is a bijection between $D(M) \times D(N)$ and $D(MN)$. □

Proposition 1. *Let p be a prime and l a positive integer. Then*

$$(a)\ D(p^l) = \{(1, d) : 1 \leqslant d \leqslant p^l\} \cup \{(p^l, 1)\} \cup$$

$$\{(p^\alpha, kp + d) : 1 \leqslant \alpha \leqslant l - 1, 1 \leqslant d \leqslant p - 1, 0 \leqslant k \leqslant p^{l-\alpha-1} - 1\};$$

$$(b)\ \mu(p^l) = p^l(1 + \frac{1}{p});$$

$$(c)\ \ \mu(N) = N\prod_{p|N}\left(1 + \left(\frac{1}{p}\right)\right).$$

Proof. (c) is immediately from (b) and Theorem 1. □

$D(MN)$ can be constructed using Algorithm 1.

Algorithm 1: $D(MN)$

(1) Construct $D(p^l)$ by Proposition 1(a);
(2) Given $D(M)$ and $D(N)$ for $(M,N)=1$, $D(MN)$ is constructed as follows. For all $(a,b)\in D(M)$,$(c,d)\in D(N)$, define $e=ac$,
$f=bN+dM-\frac{MN}{ac}([\frac{ac(bN+dM)}{MN}]'-k)$ for some $k\in\mathbb{Z}$ such that $(e,f)=1$ and $(ac,\ bN+dM-\frac{MN}{ac}([\frac{ac(bN+dM)}{MN}]'-n))\geqslant 2$ for all $0\leqslant n<k$. Then, $(e,f)\in D(MN)$ and all elements in $D(MN)$ are constructed if all pairs in $D(M)\times D(N)$ are processed.

3. The Recursive Structure of Cusps

In order to describe the cusps on $X_0(N)$, Ju. I. Manin in [2] introduced the set $\Pi(N)$, which consists of pairs of the form $[\delta;\ a \bmod (\delta,N\delta^{-1})]$. Here, δ runs through all positive divisors of N, and the second coordinate of the pair runs through any invertible class of residues modulo the greatest common divisor of δ and $N\delta^{-1}$. If $(\delta,N\delta^{-1})=1$ we sometimes put simply 1 in place of the second coordinate.

Proposition 2. *Let $\delta|N,u,v\in\mathbb{Z}$; $(u,v\delta)=(v,N\delta^{-1})=1$. The map $\mathbb{Q}\cup\{i\infty\}\to\Pi(N)$ of the form $\frac{u}{v\delta}\mapsto[\delta;\ uv \bmod (\delta,N\delta^{-1})]$ gives an isomorphism of the set of cusps on $X_0(N)$ with $\Pi(N)$.*

Proof. See Proposition 2.2 in [2]. □

In [3], (Proposition 2.2.3), J. E. Cremona gives the following characterization of cusps of $X_0(N)$.

Proposition 3. *For $j=1,2$ let $\alpha_j=p_j/q_j$ be cusps written in the lowest terms. The following are equivalent:*

(a) $\alpha_2=M(\alpha_1)$ *for some* $M\in\Gamma_0(N)$;

(b) $q_2\equiv uq_1(\bmod N)$ *and* $up_2\equiv p_1(\bmod (q_1,N))$, *with* $(u,N)=1$;

(c) $s_1q_2\equiv s_2q_1(\bmod (q_1q_2,N))$, *where s_j satisfies* $p_js_j\equiv 1(\bmod q_j)$.

Definition 2.

(a) $C_1(N)=\{(c,d):c,d\in\mathbb{Z},1\leqslant c\leqslant N,c|N,1\leqslant d\leqslant(c,Nc^{-1}),\ (c,d,Nc^{-1})=1\}$,
(b) $C(N)\ is\ defined\ in\ (2)$.

Lemma 4. *There exists a bijection between $C_1(N)$ and $C(N)$.*

Proof. It holds by $C_1(N)\subseteq D_1(N)$, $C(N)\subseteq D(N)$ and Lemma 2. □

Lemma 5. *There exists a bijection between $\Gamma_0(N)\backslash\mathbb{Q}\cup\{i\infty\}$ and $C_1(N)$.*

Proof. Let $\gamma_i=\begin{pmatrix} a_i & b_i\\ c_i & d_i\end{pmatrix},\gamma_j=\begin{pmatrix} a_j & b_j\\ c_j & d_j\end{pmatrix}\in \mathrm{SL}_2(\mathbb{Z})$ such that $(c_i,d_i),(c_j,d_j)\in D(N)$ for $1\leqslant i<j\leqslant\mu(N)$ then $\mathrm{SL}_2(\mathbb{Z})=\Gamma_0(N)\gamma_1\cup\cdots\cup\Gamma_0(N)\gamma_{\mu(N)}$ and $\Gamma_0(N)\gamma_i\neq\Gamma_0(N)\gamma_j$. $\forall c,a\in\mathbb{Z},(c,a)=1,c\geqslant 1$, let $\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ for some a,b. Then there exists $\gamma\in\Gamma_0(N),1\leqslant i\leqslant\mu(N)$ such that $\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\gamma\gamma_i$. Thus, $\begin{pmatrix} a & b\\ c & d\end{pmatrix}(\infty)=\gamma\gamma_i(\infty)$,

$\gamma(\frac{a_i}{c_i}) = \frac{a}{c}$ and $\Gamma_0(N)\frac{a}{c} = \Gamma_0(N)\frac{a_i}{c_i}$. Then, $\Gamma_0(N)\backslash\mathbb{Q}\cup\{i\infty\} = \{\Gamma_0(N)\frac{a_i}{c_i} : 1 \leqslant i \leqslant \mu(N)\}$. Define $\Phi : \Gamma_0(N)\backslash\mathbb{Q}\cup\{i\infty\} \to C_1(N)$ by

$$\Gamma_0(N)\frac{a}{c} \mapsto (c_i, d_i - (c_i, c_i^{-1}N)\left[d_i(c_i, c_i^{-1}N)^{-1}\right]'), \Gamma_0(N)\cdot i\infty \mapsto (N,1).$$

By Proposition 3, $\Gamma_0(N)\frac{a_i}{c_i} = \Gamma_0(N)\frac{a_j}{c_j}$ if $c_i d_j \equiv c_j d_i (\bmod\ (c_i c_j, N))$. Then, $c_i d_j = c_j d_i + (c_i c_j, N)h$ for some $h \in \mathbb{Z}$. Thus, $c_i = c_j$ by $c_i|N$, $c_j|N$, $(c_i, d_i) = 1$ and $(c_j, d_j) = 1$. Hence, $c_i d_j \equiv c_j d_i (\bmod\ (c_i c_j, N))$ if $d_i \equiv d_j (\bmod\ (c_i, c_i^{-1}N))$. Therefore, Φ is a bijection between $\Gamma_0(N)\backslash\mathbb{Q}\cup\{i\infty\}$ and $C_1(N)$. □

Lemma 6. *There exists a bijection between* $\Gamma_0(N)\backslash\mathbb{Q}\cup\{i\infty\}$ *and* $C(N)$.

Proof. It is immediately from Lemmas 4 and 5. □

Lemma 7. *Let* $(N_1, N_2) = 1$. *Then, there exists a bijection between* $C_1(N_1N_2)$ *and* $C_1(N_1) \times C_1(N_2)$.

Proof. Let $(c, d) \in C_1(N_1N_2)$ then $c|N_1N_2, d \leqslant (c, N_1N_2c^{-1})$, $(d, c, N_1N_2c^{-1}) = 1$. Let $c_1 = (c, N_1), c_2 = (c, N_2)$ then $c = c_1c_2, (c_1, c_2) = 1$ and $(d, c_1c_2, N_1c_1^{-1}N_2c_2^{-1}) = 1$. Thus, $(d, (c_1, N_1c_1^{-1})) = 1$, $(d, (c_2, N_2c_2^{-1})) = 1$ by $(c, N_1N_2c^{-1}) = (c_1, N_1c_1^{-1})(c_2, N_2c_2^{-1})$. Let $d_1 = d - (c_1, N_1c_1^{-1})[d(c_1, N_1c_1^{-1})^{-1}]'$ and $d_2 = d - (c_2, N_2c_2^{-1})[d(c_2, N_2c_2^{-1})^{-1}]'$ then $(d_1, (c_1, N_1c_1^{-1})) = 1$ and $(d_2, c_2, N_2c_2^{-1}) = 1$. Thus, $(c_1, d_1) \in C_1(N_1)$ and $(c_2, d_2) \in C_1(N_2)$. Define $\Phi : C_1(N_1N_2) \to C_1(N_1) \times C_2(N_2)$ by $(c, d) \mapsto ((c_1, d_1), (c_2, d_2))$.

For any $((c_1, d_1), (c_2, d_2)) \in C_1(N_1) \times C_1(N_2)$, let $c = c_1c_2$ there exists an integer d such that $d \equiv d_1(\bmod (c_1, N_1c_1^{-1}))$, $d \equiv d_2(\bmod (c_2, N_2c_2^{-1}))$ and

$$1 \leqslant d \leqslant (c_1, N_1c_1^{-1})(c_2, N_2c_2^{-1}) = (c, N_1N_2c^{-1})$$

by $((c_1, N_1c_1^{-1}), (c_2, N_2c_2^{-1})) = 1$. Thus $(c, d) \in C_1(N_1N_2)$ and hence Φ is a surjective map.

Let $\Phi((c, d)) = \Phi((c', d'))$. Then, $((c_1, d_1), (c_2, d_2)) = ((c_1', d_1'), (c_2', d_2'))$, $(c_1, d_1) = (c_1', d_1')$ and $(c_2, d_2) = (c_2', d_2')$. Thus, $c_1 = c_1', c_2 = c_2', d_1 = d_1'$ and $d_2 = d_2'$. Hence, $c = c_1c_2 = c_1'c_2' = c'$ and $d = d'$ by $d \equiv d_1(\bmod\ (c_1, N_1c_1^{-1}))$, $d \equiv d_2(\bmod\ (c_2, N_2c_2^{-1}))$, $d' \equiv d_1'(\bmod\ (c_1, N_1c_1^{-1}))$ and $d' \equiv d_2'(\bmod\ (c_2, N_2c_2^{-1}))$. Therefore, Φ is an injective map. Then Φ is a bijection between $C_1(N_1N_2)$ and $C_1(N_1) \times C_1(N_2)$. □

Theorem 2. *Let* $(N_1, N_2) = 1$. *Then, there exists a bijection between* $C(N_1N_2)$ *and* $C(N_1) \times C(N_2)$.

Proof. It is immediately from Lemmas 4 and 7. □

Proposition 4. *Let p be a prime and l a positive integer. Then,*

(a) $C(p^l) = \{(1,1), (p^l, 1)\} \cup \{(p^\alpha, kp + d) : 1 \leqslant \alpha \leqslant l-1, 1 \leqslant d \leqslant p-1, 0 \leqslant k \leqslant p^{\min\{\alpha, l-\alpha\}-1} - 1\}$;

(b) $v_\infty(p^l) = \begin{cases} (p+1)p^{\frac{l}{2}-1} & if\ \ 2|l, \\ 2p^{\frac{l-1}{2}} & otherwise; \end{cases}$

(c) $v_\infty(N) = \prod_{p|N} v_\infty(p^l)$.

Proof. (c) is immediately from (b) and Theorem 2. □

$C(N)$ can be constructed using Algorithm 2.

Algorithm 2: $C(N)$

(1) Construct $C(p^l)$ by Proposition 4(a);

(2) Let $N = N_1N_2$ for $(N_1, N_2) = 1$. Given $C(N_1)$ and $C(N_2)$. $C(N)$ is constructed as follows. For all $(c_1, d_1) \in C(N_1)$,$(c_2, d_2) \in C(N_2)$, define $c = c_1c_2$. Determinate d_0 such that $d_0 \equiv d_1(\bmod\ (c_1, N_1c_1^{-1}))$, $d_0 \equiv d_2(\bmod\ (c_2, N_2c_2^{-1}))$ and

$$1 \leqslant d_0 \leqslant (c_1, N_1c_1^{-1})(c_2, N_2c_2^{-1}).$$

Determinate $d = d_0 + \dfrac{Nk}{c}$ such that $(c, d) = 1$ and $(c, d_0 + \dfrac{Nn}{c}) \geqslant 2$ for $0 \leqslant n < k$. Then, $(c, d) \in C(N_1N_2)$ and all elements in $C(N_1N_2)$ are constructed if all pairs in $C(N_1) \times C(N_2)$ are processed.

4. The Recursive Structure of Elliptic Points of $X_0(N)$

Let $\rho = \dfrac{-1+\sqrt{3}i}{2}$. $E_2(N)$ and $E_3(N)$ are defined in (3). Then,

$$\{\frac{-d+i}{1+d^2} : (1, d) \in E_2(N)\} \ and\ \{\frac{1-2d+\sqrt{3}i}{2(1-d+d^2)} : (1, d) \in E_3(N)\}$$

are complete sets of representatives of $\Gamma_0(N)$-inequivalent elliptic points of order 2, 3, respectively.

Theorem 3. *Let $N_1, N_2 \in \mathbb{Z}, N_1, N_2 \geqslant 1$ and $(N_1, N_2) = 1$. Then*

(a) there exists a bijection between $E_3(N_1) \times E_3(N_2)$ and $E_3(N_1N_2)$;

(b) there exists a bijection between $E_2(N_1) \times E_2(N_2)$ and $E_2(N_1N_2)$.

Proof. (a) Let $(1, d_1) \in E_3(N_1)$ and $(1, d_2) \in E_3(N_2)$. Let d be the unique integer such that $d \equiv d_1 \pmod{N_1}$,$d \equiv d_2 \pmod{N_2}$ and $1 \leqslant d \leqslant N_1N_2$ then $d^2 - d + 1 \equiv 0 \pmod{N_1N_2}$. Hence, $(1, d) \in E_3(N_1N_2)$. Define

$$\Phi : E_3(N_1) \times E_3(N_2) \to E_3(N_1N_2), ((1, d_1), (1, d_2)) \mapsto (1, d).$$

Then, Φ is a bijection between $E_3(N_1) \times E_3(N_2)$ and $E_3(N_1N_2)$. The proof of (b) is similar to that of (a) and omitted. □

Proposition 5. *Let $p \in \mathbb{Z}$ be a prime and $l \in \mathbb{Z}, l \geqslant 1$. Then*

$$v_2(p^l) = \begin{cases} 0 & if\ \ p \equiv 3 \pmod 4 \ or\ 4|p^l, \\ 1 & if\ \ p = 2, \\ 2 & if\ \ p \equiv 1 \pmod 4. \end{cases}$$

Proof. Let $(1, d) \in E_2(p^l)$ then $d^2 + 1 \equiv 0 \pmod{p^l}$. Since the system of two equations $x^2 + 1 \equiv 0 \pmod p$ and $2x \equiv 0 \pmod p$ has a common solution if $p = 2$, the number of solutions of $x^2 + 1 \equiv 0 \pmod{p^l}$ is equal to that of $x^2 + 1 \equiv 0 \pmod p$ if $p \neq 2$. The cases of $p = 2$ or $4|p^l$ are trivial and we then let $p \geqslant 3$ in the following. Then, $x^2 + 1 \equiv 0 \pmod p$ has a solution if $\left(\dfrac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod 4$ by $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. In addition, $x^2 + 1 \equiv 0 \pmod p$ has two and only two solutions if it is solvable. This completes the proof. □

Proposition 6. *Let $p \in \mathbb{Z}$ be a prime and $l \in \mathbb{Z}, l \geqslant 1$. Then*

$$v_3(p^l) = \begin{cases} 0 & if \quad p \equiv 2 \pmod 3 \text{ or } 9|p^l, \\ 1 & if \quad p = 3, \\ 2 & if \quad p \equiv 1 \pmod 3). \end{cases}$$

Proof. Let $(1, d) \in E_3(p^l)$ then $d^2 - d + 1 \equiv 0 \pmod{p^l}$. Since the system of two equations $x^2 - x + 1 \equiv 0 \pmod p$ and $2x - 1 \equiv 0 \pmod p$ has a common solution if $p = 3$, the number of solutions of $x^2 - x + 1 \equiv 0 \pmod{p^l}$ is equal to that of $x^2 - x + 1 \equiv 0 \pmod p$ if $p \neq 3$. The cases of $p = 2, 3$ or $9|p^l$ are trivial and we then let $p \geqslant 5$ in the following. $x^2 - x + 1 \equiv 0 \pmod p$ has a solution if $y^2 + 3 \equiv 0 \pmod p$ has a solution by taking $x = \dfrac{y+1}{2}$ and substituting $p - y$ for y when $y \equiv 0 (\mathrm{mod} 2)$. Then, $x^2 - x + 1 \equiv 0 \pmod p$ has a solution if $\left(\dfrac{-3}{p}\right) = 1$ if $p \equiv 1 \pmod 3$ by

$$\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right), \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right), \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

and $\left(\dfrac{-3}{p}\right) = \left(\dfrac{p}{3}\right)$. In addition, $x^2 - x + 1 \equiv 0 \pmod p$ has two and only two solutions if it is solvable. This completes the proof. □

The following results are well-known, see Proposition 1.43 in [1]. However, our proof is elementary and constructive.

Corollary 2. (1) $v_2(N) = \begin{cases} 0 & if \ \ 4|N, \\ \prod_{p|N}\left(1 + \left(\dfrac{-1}{p}\right)\right) & otherwise. \end{cases}$

(2) $v_3(N) = \begin{cases} 0 & if \ \ 4|N, \\ \prod_{p|N}\left(1 + \left(\dfrac{-3}{p}\right)\right) & otherwise. \end{cases}$

Proof. It is immediately from Theorem 4, Propositions 5 and 6. □

Corollary 3. *Let $g(N)$ be the genus of the modular curve $X_0(N)$. Then, for any $(N_1, N_2) = 1$,*

$$g(N_1N_2) = 1 + \frac{\mu(N_1)\mu(N_2)}{12} - \frac{v_2(N_1)v_2(N_2)}{4} - \frac{v_3(N_1)v_3(N_2)}{3} - \frac{v_\infty(N_1)v_\infty(N_2)}{2}.$$

Proof. It is immediately from Theorems 1–3 and the formula for the genus of $X_0(N)$

$$g(N) = 1 + \frac{\mu(N)}{12} - \frac{v_2(N)}{4} - \frac{v_3(N)}{3} - \frac{v_\infty(N)}{2}.$$

□

$E_3(N)$ can be constructed using Algorithm 3.

Algorithm 3: $E_3(N)$

(1) Construct $E_3(p^l)$ by general method; (2) Let $N = N_1N_2$ for $(N_1, N_2) = 1$. Given $E_3(N_1)$ and $E_3(N_2)$. $E_3(N)$ is constructed as follows. For all $(1, d_1) \in E_3(N_1)$, $(1, d_2) \in E_3(N_2)$, Determinate d such that

$$d \equiv d_1(\text{mod } N_1), d \equiv d_2(\text{mod} N_2\ ) \textit{ and } 1 \leqslant d \leqslant N.$$

Then, $(1, d) \in E_3(N)$ and all elements in $E_3(N)$ are constructed if all pairs in $E_3(N_1) \times E_3(N_2)$ are processed.

5. Concluding Remarks

In [7], Stein mentioned that another approach to list $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ is to use that

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{p|N} \mathbb{P}^1(\mathbb{Z}/p^{v_p}\mathbb{Z}),$$

where $v_p = \text{ord}_p(N)$, and that it is relatively easy to enumerate the elements of $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ for a prime power p^n. However, this approach had never been implemented by anyone as far as I know. Thus, Algorithm 1 in this paper could be regarded as an explicit implementation of Stein's ideas. All the algorithms described in this paper have been implemented in Wolfram Language, for these Wolfram programs, see [8]. We plan to rewrite these programs in the free open-source computer algebra system SAGE and incorporate them into Stein's program [9] or Walker's program [10].

Funding: This research received no external funding.

Data Availability Statement: Not available.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Shimura, G. *Introduction to the Arithmetic Theory of Automorphic Functions*; Princeton University Press: Princeton, NJ, USA, 1971; pp. 99–103.
2. Manin, J. Parabolic points and zeta functions of modular curves. *Math.-Ussr-Izv.* **1972**, *36*, 19–66. [CrossRef]
3. Cremona, J.E. *Algorithms For Modular Elliptic Curves*; Cambridge University Press: Cambridge, UK, 1997; pp. 99–103.
4. Schoeneberg, B. *Elliptic Modular Functions: An Introduction*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2012; Volume 203, pp. 99–103.
5. Dedekind, R. Schreiben an Herrn Borchardt über die Theorie der elliptischen Modul-Functionen. *J. Reine Angew. Math.* **1877**, *83*, 265–292.
6. Weber, H. *Elliptische Functionen Und Algebraische Zahlen*; Braunschweig, F. Vieweg und Sohn: Braunschweig, German, 1891; pp. 244–245.
7. Stein, W.A. *Modular Forms, a Computational Approach*; American Mathematical Soc.: Providence, RI, USA, 2007; Volume 79, pp. 144–146.
8. Wang, S. Functions for Constructing Recursively Manin Symbols over $\mathbb{Q}$, Cusps and Elliptic Points on $X_0(N)$. 2023. Available online: https://www.wolframcloud.com/obj/1e719d22-316b-4fe1-abf1-82cc0594526a (accessed on 12 June 2023).
9. Stein, W.; The Sage Group. Modular Symbols. 2023. Available online: https://doc.sagemath.org/pdf/en/reference/modsym/modsym.pdf (accessed on 12 June 2023).
10. Walker, J. Lists of Manin Symbols over $\mathbb{Q}$, Elements of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. 2023. Available online: https://doc.sagemath.org/html/en/reference/modsym/sage/modular/modsym/p1list.html (accessed on 12 June 2023).