The representability of $\Gamma_1(N)$

1 Conventions

Let S be a scheme. Troughout this text we will call a scheme C/S a smooth curve if C is smooth of relative dimension 1, separated and finitly presented over S. This convention follows 1.2.1 of Katz and Mazur [1985]. Also if N is an integer then by N is invertible on S we mean that $N \cdot 1 \in \mathcal{O}_S(S)^*$ or equivalently that S is a $\mathbb{Z}[\frac{1}{N}]$ scheme.

2 Points of exact order N

This section is based on section 1.4 of Katz and Mazur [1985] and in this section we will define what it means to be a point of exact order N and also give some equivalent characterisations when N is invertible.
Throughout this section C/S will be a smooth curve that is also a commutative groupscheme.

Definition 2.1. Let $N > 0$ be an integer and C/S a smooth curve then a point of exact order N is a point $P \in C(S)$ such that the cartier divisor $D = \sum_{i=1}^{N} [iP]$ is a closed subgroupscheme of C.

In the above definition $[iP]$ denotes the divisor corresponding to the section iP. For D to be a subgroupscheme means that the composed map $D \times_S D \to C \times_S C \to C$ factors trough D, and similar conditions for the inverse and the unit element.

Remark. There is some caution to be taken with the above definition! If S is an $\mathbb{F}_p$ scheme then $0 \in C(S)$ is of exact order p^d for all integers d because $\ker(\mathrm{Frob}^d : C \to C^{(p^d)}) = [0]p^d$. Take for example the multiplicative group over $\mathbb{F}_p$ i.e. take $C = \mathbb{G}_{m,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[x, x^{-1}]$ then $\ker(\mathrm{Frob}^d) = (x^{p^d} - 1) = (x-1)^{p^d} = p^d[0]$.

Luckely this kind of behavior can only occur when N is not invertible on S as we can see by the following lemma.

Lemma 2.2. *Let N be invertible on S and let $P \in C(S)[N]$ then the following are equivalent.*

(1) P has exact order N

(2) For all geometric points $\operatorname{Spec} k \to S$ the point $P_k \in C_k(k)$ has exact order N.

(3) For all geometric points $\operatorname{Spec} k \to S$ the point $P_k \in C_k(k)$ has order N as an element of an abstract group.

(4) $D = \sum_{i=1}^{N}$ is etale over S

(5) The map from the constant groupscheme $(\mathbb{Z}/N\mathbb{Z})_S \to C$ given by iP on the i-th component of $(\mathbb{Z}/N\mathbb{Z})_S$ induces an isomorphism $\phi : (\mathbb{Z}/N\mathbb{Z}) \to D$.

Remark. We will proof (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3), (3) $\Leftrightarrow$ (4), (3) $\Leftrightarrow$ (5) and (5) $\Rightarrow$ (1). Only the proof of (2) $\Rightarrow$ (3) will require N to be invertible on S so without this we still have (3) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5) $\Rightarrow$ (2) $\Rightarrow$ (1). Also all proves except for (2) $\Rightarrow$ (3) will be the same. The proof of (2) $\Rightarrow$ (3) will be a different one given to me by Bas Edixhoven.

Proof.

(1)$\Rightarrow$(2) This is because being of exact order N is stable under base change.

(5)$\Rightarrow$(1) This is because the isomorphism ϕ gives D a subgroup structure.

(3)$\Leftrightarrow$(4) We know that D is locally free of rank N over S because it is a sum of N divisors of degree 1. By covering S with open affines such that their preimage in D is free we may reduce to the case $S = \operatorname{Spec} A$ and $D = \operatorname{Spec} B$ with B a free A module of rank N. Now we can see the equivalence as follows:

B is etale over $A \Leftrightarrow Discr_{B/A} \in A^* \Leftrightarrow \forall A \to k$ with k an algebraically closed field: $Discr_{B/A} \neq 0 \in k^* \Leftrightarrow \forall A \to k$: D_k is etale over $\operatorname{Spec} k \Leftrightarrow$ (3)

(3)⇔(5) Again reduce to the case $S = \operatorname{Spec} A$ and $D = \operatorname{Spec} B$ with B a free A module of rank N. Since $(\mathbb{Z}/N\mathbb{Z})_S$ is also free of rank N over S we can write $\phi = M$ for some matrix $M \in \mathbf{M}_N(A)$ after choosing a basis on both sides. Now the equivalence is shown as follows:

ϕ is an isomorphism $\Leftrightarrow \det M \in A^* \Leftrightarrow \forall A \to k$ with k an algebraically closed field: $\det M \neq 0 \in k \Leftrightarrow$ (3).

(2)⇒(3) Let (2) hold and asume for contradiction that (3) doesn't hold for a certain $\operatorname{Spec} k \to S$ then there is a $1 < d < N$ with $dP_k = 0$ in the rest of the proof we assume that d is as small as possible. Then the divisor $D' = (N/d)[0]$ is the connected component of the identity in D and hence D' is a subgroupscheme of D. Now as a scheme $D' \cong \operatorname{Spec} k[x]/(x^{N/d})$. From Jinbi his talk we have seen that the fact that D' is a groups scheme implies that

$$\Omega^1(k[x]/(x^{N/d})) = \frac{k[x]/(x^{N/d})dx}{N/D^{N/d-1}}$$

is a free $k[x]/(x^{N/d})$ module. But since $N/d \neq 1$ this can only happen if $N/d = 0 \in k$ wich is a contradiction.

□

3 The category $\mathrm{Ell}_{/T}$ and moduli problems

In this section we discus some formalism of what we exactly mean by a moduli problem. What we do here is similar to the definitions given in Jinbi his talk, but slightly more precise so that we can later clearly state the main theorem we will prove in the section 4.

Definition 3.1. Let T be a scheme then we define the category $\mathrm{Ell}_{/T}$ to be the category whose objects are triples (E, S, f) where S is a T scheme, E is an elliptic curve over S and $f : E \to S$ is the defining morphism that makes E an elliptic curve over S. A morphism between triples $g : (E_1, S_1, f_1) \to (E_2, S_2, f_2)$ is a pair $g = (g_1, g_2)$ with $g_1 : E_1 \to E_2$ and $g_2 : S_1 \to S_2$ a morphisms such that the following diagram is cartesian:

$$\begin{array}{ccc} E_1 & \xrightarrow{g_1} & E_2 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ S_1 & \xrightarrow{g_2} & S_2 \end{array}$$

Note that the notation (E, S, f) is quite cumbursome so instead we will write E/S for this object if it is clear what f is. We will also write Ell for $\mathrm{Ell}_{/\operatorname{Spec}\mathbb{Z}}$.

Definition 3.2. A moduli problem is a contravariant functor $\mathcal{P} : \mathrm{Ell} \to \mathrm{Sets}$. Let T be a scheme, then we call $\mathcal{P}$ representable over T if the functor $\mathcal{P}|_{\mathrm{Ell}_{/T}}$ is representable. If $\mathcal{P}$ representable over T then we will similarly call a pair $(E/S, P)$ with $E/S \in \mathrm{Ell}_{/T}$ and $P \in \mathcal{P}(E/S)$ universal for $\mathcal{P}$ over T if $(E/S, P)$ is universal for $\mathcal{P}|_{\mathrm{Ell}_{/T}}$.

For more details on universal pairs and their relation to representability see Appendix A or Mac Lane [1998][Chapter III]

To make the above defintions more concrete we aply it to the examples Jinbi gave.

Example 1. Let $\Gamma_\omega : \mathrm{Ell} \to \mathrm{Sets}$ be the moduli problem given by $\Gamma_\omega(E/S) := \{\omega \in \omega_{E/S}(S) | \omega \text{ generates } \omega_{E/S}\}$. Then we have seen that Γ_ω is reprentable over $\mathbb{Z}[\frac{1}{6}]$. Let $\Delta = -16(4a^3 - 27b^2)$, $A = \mathbb{Z}[\frac{1}{6}, a, b, \frac{1}{\Delta}]$, $Y_\omega = \operatorname{Spec} A$ and $E_\omega = \operatorname{Proj} A[x, y, z]/(y^2z - x^3 - axz^2 - bz^3)$ then the section $-\frac{dx}{2y} = -\frac{dy}{3x^2+a}$ of $\Omega^1_{E_\omega/Y_\omega}(D_{E_\omega}(Z))$ will extend to a global section $\Omega_{univ} \in \Omega^1_{E_\omega/Y_\omega}(E_\omega)$. Now take $\omega_{univ} := 0^*(\Omega_{univ}) \in 0^*(\Omega^1_{E_\omega/Y_\omega})(Y_\omega) = \omega_{E_\omega/Y_\omega}(Y_\omega)$ [1] then the pair $(E_\omega/Y_\omega, \omega_{univ})$ is universal for Γ_ω over $\mathbb{Z}[\frac{1}{6}]$.

Example 2. Let $\Gamma_{\geq}(4) : \mathrm{Ell} \to \mathrm{Sets}$ be the moduli problem given by

$$\Gamma_{\geq}(4)(E/S) :=$$

$$\{P \in E(S) | P_k \text{ has order 4 or more for all geometric points } \operatorname{Spec} k \to S\}.$$

Then we have seen that $\Gamma_{\geq}(4)$ is reprentable over $\mathbb{Z}$. Let $\Delta = -t^3(16t^2 + (8s^2 - 20s - 1)t + s(s+1)^3)$, $A = \mathbb{Z}[s, t, \frac{1}{\Delta}]$, $Y_{\geq}(4) = \operatorname{Spec} A$ and $E_{\geq}(4) =$

[1] We could also define $\omega_{univ} : f_*(\Omega_{univ}) \in f_*(\Omega^1_{E_\omega/Y_\omega})(Y_\omega) = \omega_{E_\omega/Y_\omega}(Y_\omega)$, wich actually is the same element under the cannonical identifiaction $0^*(\Omega^1_{E_\omega/Y_\omega}) = f_*(\Omega^1_{E_\omega/Y_\omega})$

Proj $A[x,y,z]/(y^2+(s+1)xy+ty-x^3-tx^2)$ then $P_{\geq}(4)=(0:0:1)\in E_{\geq}(4)(Y_{\geq}(4))\subset \mathbb{P}^2_{Y_{\geq}(4)}(Y_{\geq}(4))$ has order 4 or more for all geometric points and in fact the pair $(E_{\geq}(4)/Y_{\geq}(4), P_{\geq}(4))$ is universal for $\Gamma_{\geq}(4)$.

To a moduli problem on Ell we can also associate a functor on Sch in the following way.

Definition 3.3. Let $\mathcal{P}:\text{Ell}\to\text{Sets}$ be a moduli problem and T be a scheme then we define $\mathcal{P}|_{\text{Sch}/T}:\text{Sch}/T\to\text{Sets}$ by

$$S\mapsto\left\{\begin{array}{c}\text{set of isomorphism classes of pairs } (E,a)\\ \text{where } E \text{ is an elliptic curve over } S \text{ and } a\in\mathcal{P}(E/S)\end{array}\right\}$$

where a morphism between pairs (E_1,a_2) and (E_2,a_2) is a morphism $g: E_1\to E_2$ such that $\mathcal{P}(g)(a_2)=a_1$.

And the representability of $\mathcal{P}|_{\text{Sch}/T}$ follows from the representability of mp over T. To be precise:

Proposition 3.4. *If $(E/S,a)$ is a universal pair for $\mathcal{P}$ over T then $(S,(E,a))$ is a universal pair[2] for $\mathcal{P}|_{\text{Sch}/T}$.*

Proof. By defintion we know that $\Psi^{(E/S,a)}$ has an inverse (see definition 3.2) let $\Psi^{(E/S,a)^{-1}}$ be this inverse. Then we define $\Psi^{(S,(E,a))^{-1}}:\mathcal{P}|_{\text{Sch}/T}\to \text{Hom}_T(\_,S)$ componentwise as:

$$\Psi^{(S,(E,a))^{-1}}_{S'}:\mathcal{P}|_{\text{Sch}/T}(S')\to\text{Hom}_T(S',S) \quad (1)$$
$$(E',a')\mapsto g_2 \quad (2)$$

Where g_2 is the second component of the morphism $\Psi^{(E/S)^{-1}}_{E'/S'}(a'):E'/S'\to E/S$. One can show that this really is an inverse of $\Psi^{(S,(E,a))}$ showing that $(S,(E,a))$ is universal. □

4 The representability of $\Gamma_1(N)$

In this section we will study the following set of moduli problems.

[2]The definition of universal pair here is similar to that in definition 3.2 and this concept of universal pair is in fact purely category theoretical.

Definition 4.1. Let $N \geq 1$ be an integer then we define the moduli problem $\Gamma_1(N) : \text{Ell} \to \text{Sets}$ by

$$\Gamma_1(N)(E/S) := \{P \in E(S) | P \text{ has exact order } N\}$$

if $\Gamma_1(N)$ is representable over T then we will write $(E_1(N)_T/Y_1(N)_T, P_1(N)_T)$ for a corresponding universal pair.

Note that for a fixed N such that $\Gamma_1(N)$ is representable there will be multiple universal pairs, but they are unique up to unique isomorphism so it will not be a to big abuse of notation, and in fact later on we will explicitly construct one of them, so one might instead take that as the definition of $(E_1(N)_T/Y_1(N)_T, P_1(N)_T)$ from that point on.

The main theorems we will prove are.

Theorem 4.2. *If $N \geq 4$ then $\Gamma_1(N)$ is reprentable over $\mathbb{Z}[\frac{1}{N}]$.*

and

Theorem 4.3. *If $N \geq 4$ then $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is curve a over $\mathbb{Z}[\frac{1}{N}]$ i.e smooth of relative dimension 1 separated and of finite presentation.*

Actually there is also a converse to Theorem 4.2 for $N < 4$

Proposition 4.4. *If $N = 1, 2$ or 3 and T is a scheme wich has a geometric point $\operatorname{Spec} k \to T$ with $\operatorname{char} k \neq 2, 3$ then $\Gamma_1(N)|_{\text{Sch}/T}$ is not representable and hence $\Gamma_1(N)$ is not representable over T.*

This proposition can also be proven without the condition $\operatorname{char} k \neq 2, 3$ but it will really complicate computations.

Proof. Define E_a be the elliptic curve over $k(t)$ given by the equation $y^2 - x^3 - a$ for any $a \in k(t)^*$. Now all isomorphims between elliptic curves over $k(t)$ in weierstrass form are of the form $\phi_{u,r,s,t}(x, y) = (u^2x + r, u^3y + su^2x + t)$[3] for some u, r, s, t in $k(t)$.Let a, b in $k(t)^*$ and let $\phi_{u,r,s,t} : E_a \to E_b$ be an isomorphism then by putting $(u^2x + r, u^3y + su^2x + t)$ in the eqation of E_b it's easy to see that $r = s = t = 0$. Doing this will also give $0 = (u^3y)^2 - (u^2x)^3 - b = u^6(y^2 - x^3) - b = u^6a - b$ hence $E_a \cong E_b$ if and only if $a/b \in k(t)^{*6}$. From this discussion it's easy to see that E_1 E_{t^2},E_{t^3} are not isomorphic over $k(t)$. Suppose for contradiction that $\Gamma_1(N)|_{\text{Sch}/T}$ is reprentable and let $Y_1(N)_T$

[3]This can be deduced from Jinbi's talk about elliptic curves in weierstrass form.

be the scheme representing it. Then the cannonical map $Y_1(N)_T(k(t)) \to Y_1(N)_T(\overline{k(t)})$ will be an injection. However for $N = 1$ the fact that $(E_1, (0 : 1 : 0))$ and $(E_{t^2}, (0 : 1 : 0))$ are not isomorphic but become isomorphic over $\overline{k(t)}$ will show that $Y_1(1)_T(k(t)) \to Y_1(1)_T(\overline{k(t)})$ is not an injection, contradicting our assumption hence $\Gamma_1(1)|_{\mathrm{Sch}/T}$ is not representable. For $N = 2$ and one can apply the same reasoning using the pairs $(E_1, (-1 : 0 : 1))$ and $(E_{t^3}, (-t : 0 : 1))$ and for $N = 3$ one can use the pairs $(E_1, (0 : 1 : 1))$ and $(E_{t^2}, (0 : t : 1))$. □

Remark. The proof above also gives some insight in why $\Gamma_1(N)$ is not nececarily representable over $\mathbb{Z}$. Because if we take for example $\Gamma_1(p^n)$ with $p > 3$ a prime then we have seen that $(0 : 1 : 0)$ is a point of exact order p^n for all elliptic curves E/S with S an $\mathbb{F}_p$ scheme. Hence we can use the pairs $(E_1, (0 : 1 : 0))$ and $(E_{t^2}, (0 : 1 : 0))$ above to show that $\Gamma_1(p^n)$ is not representable. This would be an argument to use item (3) of lemma 2.2 as the definition of exact order N. However this will make the resulting moduli space $Y_1(N)$ less usefull for studying the arithmetic of for example elliptic curves over numberfields wich have point of order p that reduce to point of order 1. Similarly the the moduli space $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ doesn't allow us to easilly study elliptic curves over numberfields wich have bad reduction at a certain prime. This second problem can be fixed by generalizing the definition of elliptic curve a bit and construct a new moduli space $X_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ wich will hopefully happen later in this seminar.

4.1 Proof of theorem 4.2

We will proof this theorem by showing that $\Gamma_1'(N)$ is representable over $\mathbb{Z}$ where $\Gamma_1'(N)$ is the moduli problem we get by replacing being of exact order N by item (3) of lemma 2.2. We do this be explicitly contructing a universal pair for $\Gamma_1'(N)$. Since N is invertible in $\mathbb{Z}[\frac{1}{N}]$ we see that $\Gamma_1'(N)|_{\mathrm{Ell}/\mathbb{Z}[\frac{1}{N}]}$ and $\Gamma_1(N)|_{\mathrm{Ell}/\mathbb{Z}[\frac{1}{N}]}$ are acutally the same functor so the theorem will follow.

Now define the moduli problem $\Gamma_{\geq}(N)$ similar to $\Gamma_{\geq}(4)$ in example 2.

Proposition 4.5. *Let $N \geq 4$ then $\Gamma_{\geq}(N)$ is representable by a universal pair $(E_{\geq}N/Y_{\geq}(N), P_{\geq}(N))$ with $Y_{\geq}(N) \subset Y_{\geq}(4)$ an open subcheme.*

Proof. Since $Y_{\geq}(4) \subset \mathbb{A}^2_{\mathbb{Z}}$ open and $\operatorname{Pic}\mathbb{A}^2_{\mathbb{Z}} = 0$ we see that $\operatorname{Pic} Y_{\geq}(4) = 0$ so for all $d \in \mathbb{Z}$ we can write $dP_{\geq}(4) = (s_{d,0} : s_{d,1} : s_{d,2})$ with $s_{d,i} \in$

$\mathcal{O}_{Y_{\geq}(4)}(Y_{\geq}(4))$. Now define

$$Y_{\geq}(N) := \bigcap_{d=1}^{N-1} (D_{Y_{\geq}(N)}(s_{d,0}) \bigcup D_{Y_{\geq}(N)}(s_{d,2})$$

Then this will be an open subcheme of $Y_1(4)$. Define $E_{\geq}4 := f^{-1}(Y_{\geq}(N)) = E_{\geq}4 \times_{Y_{\geq}(4)} Y_{\geq}(N)$ and $P_{geq}(N) = P_{geq}(4)|_{Y_{\geq}(N)}$. $P_{\geq}(N)$ will have order at least N in all geometric points since for all $d < N$ and all geometric points $\operatorname{Spec} k \to Y_{\geq}(N)$ we have $dP_{geq}(N)_k \neq (0:1:0)$ by construction. Now let $(E/S, P)$ be any pair of an elliptic curve together with a point of order at least N then P is of order at least 4 so we get a unique morphism $g : E/S \to E_{\geq}(4)/Y_{\geq}(4)$. Now by contsruction g will factor trough $E_{\geq}(N)/Y_{\geq}(N)$ and because $E_{\geq}(N)/Y_{\geq}(N) \to E_{\geq}(4)/Y_{\geq}(4)$ is given by a pair of open immersions, this factorisation is even unique hence we have shown that the pair $(E_{\geq}N/Y_{\geq}(N), P_{\geq}(N))$ is universal for $\Gamma_{\geq}(N)$. □

Now define $Y_1'(N) := Z(s_{d,0}, s_{d,2}) \subset Y_{\geq}(N)$ to be the closed subscheme defined by the ideal sheaf generated by $s_{d,0}$ and $s_{d,2}$ and define $E_1'(N)$ and $P_1'(N)$ by $(E_1'(N), P_1'(N)) := \Gamma_{\geq}(N)_{\mathrm{Sch}}(Y_1'(N) \to Y_{\geq}(N))(E_{\geq}(N), P_{\geq}(N))$. Using the exact same argument as in the proof above but replacing open immersion by closed immersion we see that the pair $(E_1'(N)/Y_1'(N), P_1'(N))$ is indeed universal. □

Remark. Using division polynomials one can even find a single $f_d \in \mathcal{O}_{Y_{\geq}(4)}(Y_{\geq}(4))$ such that $D_{Y_{\geq}(N)}(f_d) = (D_{Y_{\geq}(N)}(s_{d,0}) \cup D_{Y_{\geq}(N)}(s_{d,2})$. For more details on division polynomials in a scheme theoretic setting see for example in Jinbi Jin his thesis Jin [2011]. As a corollary we get that $Y_{\geq}(N)$ and $Y_1'(N)$ are actually affine. It is also possible to prove that $Y_1'(N)_{\mathbb{Z}[\frac{1}{N}]} = Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is affine without using division polynomials and we will give a sketch how to do this in 4.2.

Example 3. As an example we give $Y_1(4)_{\mathbb{Z}[\frac{1}{4}]}$ and $Y_1(5)_{\mathbb{Z}[\frac{1}{5}]}$ explicitly. The

points $dP_{\geq}(4)$ are the following [4]:

$$\begin{aligned} P_{geq}(4) =&(0:0:1) && (3)\\ 2P_{geq}(4) =&(-t:st:1) && (4)\\ 3P_{geq}(4) =&(-s:s-t:1) && (5)\\ 4P_{geq}(4) =&((t-s)ts:st^2(1-s)-t^3:s^3) && (6)\\ 5P_{geq}(4) =&((s^3t-st(s-t))(s-t):s^2t^(s-t)-s^5t:(s-t)^3) && (7) \end{aligned}$$

From this we see that $Y_1(4)_{\mathbb{Z}[\frac{1}{4}]} = \operatorname{Spec}\mathbb{Z}[\frac{1}{4},s,t,\frac{1}{\Delta}]/((t-s)ts,s^3) = \operatorname{Spec} A$ Now since $s^3 = 0 \in A$ we see that $(t-s)t$ is a unit in A because s is nilpotent and t a unit. In particular we see that $s = 0$ in A hence $A = \operatorname{Spec}\mathbb{Z}[\frac{1}{4},s,t,\frac{1}{\Delta}]/(s)$ in particular we see that $Y_1(4)_{\mathbb{Z}[\frac{1}{4}]}$ is smooth of relative dimension 1 over $\mathbb{Z}[\frac{1}{4}]$. Similarly one shows that $Y_1(5)_{\mathbb{Z}[\frac{1}{5}]} = \operatorname{Spec}\mathbb{Z}[\frac{1}{5},s,t,\frac{1}{\Delta}]/(s-t)$ is smooth of relative dimension 1 over $\mathbb{Z}[\frac{1}{5}]$

4.2 Ingredients of the proof of theorem 4.3

Before we can proof that $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is a curve over $\mathbb{Z}[\frac{1}{N}]$ we need to develop some more theory. We state proposition 10.1.2 from Edixhoven [1996] and we will give a modified proof.

Proposition 4.6. *Let $f : X \to Y$ be a finite etale morphism of schemes and let $p : Y \to X$ be a section then* im *is open and closed in X and hence $X = \operatorname{im} p \amalg (Y \setminus \operatorname{im} p)$ as schemes.*

Proof. By covering Y with open affines we can reduce to the case that $Y = \operatorname{Spec} A$ is affine. Then also $X = \operatorname{Spec} B$ is affine and since f is finite etale, B is a finitely generated as A module. Now define $I = \ker p^{\#}$ and let $\pi : B \to B/I^2$ be the quotient map then I claim $I = I^2$. Indeed since f is etale it is also formally etale hence the following diagram has a unique diagonal that makes everything commute:

$$\begin{array}{ccc} A & \xrightarrow{\pi\circ f} & B/I^2 \\ \downarrow{\scriptstyle f} & \exists! \nearrow & \downarrow \\ B & \longrightarrow & B/I = A \end{array}$$

[4] I computed these with sage and written them down in a slightly nicer form

Since both π and $\pi \circ f \circ p$ make the diagram commute they are equal hence $I^2 = \ker \pi = \ker \pi \circ f \circ p \supset I$ so $I = I^2$ as claimed. Now since the exact sequence of A-modules $I \to B \to A$ is split we see that $B \cong A \oplus I$ as A-modules. Since B is finitely generated as A module we see that I is also finitely generated as an A-module and hence also finitely generated as a B module. Now Nakayama's lemma gives us that there is an r in B such that $r \equiv 1 \mod I$ and $rI = 0$. Since $(r, r-1) = (1)$ we have $I = (r-1)I + r(I) = (r-1)I \subset (r-1)B \subset I$ hence $I = (r-1)$ and by the chinese remainder theorem we have $B \cong B/r \times B/(r-1) = R/r \times A$ and we have found the wanted decomposition. □

Corollary 4.7. *Let S be a scheme, E/S an elliptic curve and d, N be two integers with $d|N$ and N is invertible on S then $E[d]$ is open and closed in $E[N]$ and $E[N] = E[d] \amalg (E[N] \backslash E[d])$*

Proof. We have that $E[N/d]$ is etale over S and that 0 is a section so $E[N/d] = \operatorname{im} 0 \amalg (E[N/d] \backslash \operatorname{im} 0)$ hence applying the inverse of the multiplication by d map we get $E[N] = [d]^(- 1)(\operatorname{im} 0 \amalg (E[N/d] \backslash \operatorname{im} 0)) = E[d] \amalg (E[N] \backslash E[d])$ □

By the above corollary it makes sense to make the following definition:

Definition 4.8. Let E/S and N be as in the previous corollary then we define:

$$E[N]^* := E[N] \backslash \bigcup_{d|N, d<N} E[d]$$

We see that $E[N]^*$ is an open and closed subscheme of $E[N]$ and in particular that it is etale over S. And also by construction it is clear that giving an S point of $E[N]^*$ is equivalent to giving a point of exact order N in $E(S)$.

Now I will sketch the proof that $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is affine as promised in 4.1.

Proof. The key point is to note that $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]} = P_{\geq}(4)^{-1}(E_{\geq}(4)[N]^*)$ as they represent the same functor. Then the composition $E_{\geq}(4)_{\mathbb{Z}[\frac{1}{N}]}[N]^* \to E_{\geq}(4)_{\mathbb{Z}[\frac{1}{N}]}[N] \to E_{\geq}(4)_{\mathbb{Z}[\frac{1}{N}]}$ is a sequence of closed immersions hence itself a closed immersion. This shows $P_{\geq}(4)^{-1}(E_{\geq}(4)[N]^*) \to Y_{\geq}(N)$ is a clossed immersion, hence $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is closed in affine hence affine itself. □

Proposition 4.9. *Let M, N be coprime integers with $N \geq 4$ then the schemes $E_1(N)_{\mathbb{Z}[\frac{1}{NM}]}[M]^*$ and $Y_1(NM)_{\mathbb{Z}[\frac{1}{NM}]}$ are isomorphic.*

One might simply say that both schemes represent the same functor and hence are isomorphic. And the proof below is basically a spelled out version of that remark.

Proof. In this proof we drop all the $\mathbb{Z}[\frac{1}{NM}]$ for readability. Let $E/E_1(N)[M]^*$ be the elliptic curve $E_1(N)[M]^* \times_{Y_1(N)} E_1(N)$ and consider the following cartesian diagram.

$$\begin{array}{ccc} E & \longrightarrow & E_1(N) \\ \downarrow & & \downarrow \\ E_1(N)[M]^* & \longrightarrow & Y_1(N) \end{array}$$

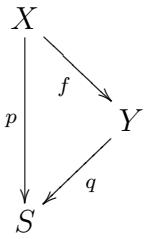
. Let $s : E/E_1(N)[M]^* \to E_1(N)/Y_1(N)$ be the morphism in Ell corresponding to this diagra and let $i : E_1(N)[M]^* \to E_1(N)$ be the inclusion then $P := P_1(N)_{E_1(N)[M]^*} \in E(E_1(N)[M]^*)$ is a point of exact order N and $Q := (\mathrm{Id}_{E_1(N)[M]^*}, i) \in inE(E_1(N)[M]^*)$ is point of exact order M hence $P + Q$ is of exact order NM (here we use the isomorphism $M\mathbb{Z}/NM\mathbb{Z} \times N\mathbb{Z}/NM\mathbb{Z} \to \mathbb{Z}/NM\mathbb{Z}$ given by $(a, b) \mapsto a + b$). And $P + Q$ will give us a morphism from $g : E/E_1(N)[M]^* \to E_1(NM)/Y_1(NM)$. Now to get an inverse of this morphism consider the point $P_1(NM)$ of exact order NM in $E_1(NM)/Y_1(NM)$. Using the inverse of $M\mathbb{Z}/NM\mathbb{Z} \times N\mathbb{Z}/NM\mathbb{Z} \to \mathbb{Z}/NM\mathbb{Z}$ we get points $P, Q \in E_1(NM)(Y_1(NM))$ of exact order N and M respectively. The point P will give us a morphism $h : E_1(NM)/Y_1(NM) \to E_1(N)/Y_1(N)$ and the point Q will give a factorisation $g^{-1} : E_1(NM)/Y_1(NM) \to E/E_1(N)[M]^*$ of h $E/E_1(N)[M]^*$ such that $h = g^{-1} \circ s$. One can check that g and g^{-1} are indeed eachothers inverse and the proposition follows. □

Proposition 4.10. *The map $f : E_1(N)_{\mathrm{Spec}[\frac{1}{NM}]}[M]^* \to Y_1(N)_{\mathbb{Z}[\frac{1}{NM}]}$ is surjective (as map of sets).*

Proof. Let $p \in Y_1(N)_{\mathbb{Z}[\frac{1}{NM}]}$ be point and let $s : \mathrm{Spec}\, k \to Y_1(N)_{\mathbb{Z}[\frac{1}{NM}]}$ be a geometric point that maps to p. Then it suffices to show that we can find an $s' : \mathrm{Spec}\, k \to E_1(N)_{\mathrm{Spec}[\frac{1}{NM}]}[M]^*$ such that $f \circ s' = f$. But such an s' is just an element of $E_1(N)[M]^*(k)$ then because k has characteristic unequal to M we know that $E_1(N)[M](k) = E_1(N)(k)[M] \cong (\mathbb{Z}/MZ)^2$ so such an s' exists. □

The last result wich we need is[Stacks Project, 2012, Lemma 02K5] wich we state below without proof.

Lemma 4.11. *Let*



be a commutative diagram of morphisms of schemes. Assume that

1. *f is surjective, and smooth,*
2. *p is smooth, and*
3. *q is locally of finite presentation*[5].

Then q is smooth.

We need this for the following corollary

Corollary 4.12. *If aditionally f is etale and p smooth of relative dimension* 1 *then q is smooth of relative dimension* 1.

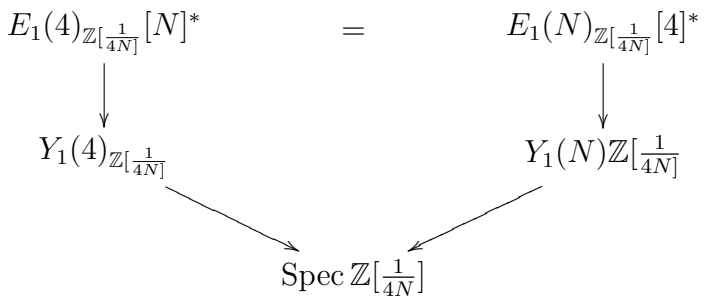
5 proof of theorem 4.3

We also have that $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is of finite presentation by construction, it is also separated because it is affine[6]. So we only have to show that it $Y_1(N)_{\mathrm{Spec}[1N]}$ is smooth of relative dimension 1 over $\mathbb{Z}[\frac{1}{N}]$. Now we have seen in example 3 that the theorem is true for $N = 4, 5$. First we are going to proof the theorem

[5]In fact this is implied by (1) and (2). Also it suffices to assume f is surjective, flat and locally of finite presentation, see the stacks project for more details.

[6]We can also say that it is separated because the map to $Y_{\geq}(4)$ can be written as a closed immersion followed by an open immersion and the latter space if affine. In this we don't use that $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is affine.

only for $N \geq 4$ and N coprime to 10. Now consider the commutative diagram:



Now the composition of the leftmost two maps is smooth of relative dimension 1 because one is smooth of relative dimension 1 and the other etale. Also the top right map is etale and surjective. So we can apply corrollary 4.12 to see that $Y_1(N)\mathbb{Z}[\frac{1}{4N}]$ is smooth or relative dimension 1 over $\operatorname{Spec}\mathbb{Z}[\frac{1}{4N}]$. Repeating the argument with 4 replaced by 5 we see that $Y_1(N)\mathbb{Z}[\frac{1}{5N}]$ is smooth or relative dimension 1 over $\operatorname{Spec}\mathbb{Z}[\frac{1}{5N}]$ so as a conclusion we see that $Y_1(N)\mathbb{Z}[\frac{1}{N}]$ is smooth or relative dimension 1 over $\operatorname{Spec}\mathbb{Z}[\frac{1}{N}]$. Now that we have seen that the theorem is true for all integers coprime to 10 and bigger then 4 we can proof it for arbitrary $N \geq 4$ by chosing primes $p, q > N$. We know that the theorem is true for p, q so repeating the argument above by replacing 4 by p and 5 by q the full theorem follows.

A Universal pairs and representability

This section is a reformulation of a small part of the theory in Mac Lane [1998][Chapter III] in terms contravariant functors and without the explicit mention of comma category or universal arrow. The goals is to discuss the link between universal pairs and representation of a functor.

Definition A.1. Let C be a category and $K : C \to Sets$ a contrariant functor. Then we define the category $(* \downarrow K)$ to be the category wich has object pairs (c, s) with $C \in K$ an object and $s \in K(c)$ an element. The morphisms $g : (c_1, s_1) \to (c_2, s_2)$ $(* \downarrow K)$ are morphisms $g : c_1 \to c_2$ in C such that $K(g)(s_2) = s_1$. A universal pair for K is a terminal object in the category $(* \downarrow K)$.

Definition A.2. Let C be a category with small homsets [7] and $K : C \to Sets$ a contrariant functor. Then a representation of K is a pair (r, ϕ) with $r \in K$ an object and $\phi : \hom_C(,r) \to K$ a natural isomorphism. The object r is called the representing object and K is called representable if such a representation exist.

The proposition below is the reason for this appendix and is basically proposition III.2 from Mac Lane [1998]

Proposition A.3. *Let C be a category with small homsets and $K : C \to$ Sets a contravariant functor. If (c, s) is a universal pair for K then the natural transformation $\phi : \hom_C(,c) \to K$ whose compenent at $d \in C$ is given by*

$$\phi_d : \hom_C(d, c) \to K(d) \tag{8}$$

$$g \mapsto K(g)(s) \tag{9}$$

is a representation of K and every representation of K is obtained from exactly one universal pair.

References

Bas Edixhoven. Varietes jacobiennes, lecture notes, 1996. URL `http://www.math.leidenuniv.nl/~edix/public_html_rennes/cours/dea9596.h%tml`.

[7] Small homsets are a technicality to be able to formulate category theory in set theory. At your will you can either ignore this or consult Mac Lane [1998] for more details

Jinbi Jin. Point counting formulae on universal elliptic curves. Master's thesis, Universiteit Leiden, 2011. URL `http://www.math.leidenuniv.nl/nl/theses/282/`.

Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves. (AM-108) (Annals of Mathematics Studies)*. Princeton University Press, 1985. ISBN 0691083525.

Saunders Mac Lane. *Categories for the Working Mathematician (Graduate Texts in Mathematics)*. Springer, 1998. ISBN 0387984038.

The Stacks Project. Stacks Project, 2012. URL `http://math.columbia.edu/algebraic_geometry/stacks-git`.