René Schoof
Dipartimento di Matematica
2^{a} Università di Roma "Tor Vergata"
I-00133 Roma ITALY
Email: schoof@wins.uva.nl

Abelian varieties over the field of the 20th roots of unity that have good reduction everywhere

Abstract. The elliptic curve E given by $Y^2 + (i+1)XY + iY = X^3 + iX^2$ acquires good reduction everywhere over the cyclotomic field $\mathbf{Q}(\zeta_{20})$. We show, under assumption of GRH, that every abelian variety over $\mathbf{Q}(\zeta_{20})$ with good reduction everywhere is isogenous to E^g for some $g \geq 0$.

1. Introduction.

For $f = 1, 3, 4, 5, 7, 8, 9$ and 12 there do not exist any abelian varieties over the cyclotomic field $\mathbf{Q}(\zeta_f)$ that have good reduction modulo every prime. Under assumption of the Generalized Riemann Hypothesis (GRH) the same can be proved for $\mathbf{Q}(\zeta_{11})$ and $\mathbf{Q}(\zeta_{15})$. These are the main results of [6]. For all other conductors f there do exist abelian varieties over $\mathbf{Q}(\zeta_f)$ with good reduction everywhere.

The techniques of [6] still give substantial information about abelian varieties with good reduction everywhere over cyclotomic fields that are not in this list. Ordering the fields with respect to their root discriminants, the first field not in the list is $\mathbf{Q}(\zeta_{20})$. Over this field the elliptic curve E given by the equation

$$Y^2 + (i+1)XY + iY = X^3 + iX^2.$$

has good reduction everywhere. This can be seen as follows. The discriminant of the equation is equal to $-(1+2i)^3$. Therefore E has good reduction outside the prime $1+2i$ of the ring $\mathbf{Z}[i]$. Since the reduction at $1+2i$ is of Kodaira type III, the curve E acquires good reduction everywhere over any Galois extension of $\mathbf{Q}(i)$ for which the ramification indices of the primes over $1+2i$ are divisible by 4. In particular, E acquires good reduction everywhere over $\mathbf{Q}(\zeta_{20})$.

The main result of this paper is the following.

Theorem 1.1. *(GRH) Every abelian variety over $\mathbf{Q}(\zeta_{20})$ that has good reduction everywhere is isogenous to a power of E.*

The theorem is proved under assumption of the Generalized Riemann Hypothesis (GRH) for zeta functions of number fields. The main ingredients are the results of [6]. See [5] for a similar result, proved without assuming GRH, for abelian varieties over $\mathbf{Q}(\sqrt{6})$.

The proof of the theorem proceeds by analyzing finite flat commutative group schemes of 2-power order over the ring $\mathbf{Z}[\zeta_{20}]$. We deduce that the 2-divisible group associated to any abelian variety A over $\mathbf{Q}(\zeta_{20})$ with good reduction everywhere is isogenous to the 2-divisible group associated to E^g for some $g \geq 0$. Faltings's isogeny theorem implies then that the abelian varieties A and E^g are isogenous over $\mathbf{Q}(\zeta_{20})$.

2. 2-group schemes over $\mathbf{Z}[\zeta_{20}]$.

Let F denote the number field $\mathbf{Q}(\zeta_{20})$ and let $O_F = \mathbf{Z}(\zeta_{20})$. In this section we study finite flat commutative group schemes of 2-power order over the ring O_F or 2-*group schemes* for short. Finite flat group schemes of order 2 are examples of 2-group schemes. Since (2) is the square of the prime ideal generated by $1+i$ in O_F, it follows from the discussion on the first page of the paper by Oort and Tate [8] there are three of these. Apart from the group schemes $\mathbf{Z}/2\mathbf{Z}$ and μ_2, there is an order 2 group scheme that is local-local at the prime 2. It can be described as follows. The elliptic curve E of section 1 has j-invariant 1728 and endomorphism ring isomorphic to $\mathbf{Z}[i]$. The kernel $E[f]$ of the endomorphism $f = 1 + i$ in the ring $\mathrm{End}(E)$ is a finite flat group scheme of order 2. Its Hopf algebra is isomorphic to $O_F[T]/(T^2 - (1+i)T)$ with group law $t + t' - (i-1)tt'$.

Group schemes of order 2 are *simple*. Under assumption of GRH, the converse is true over the ring O_F.

Theorem 2.1. *(GRH) The only simple 2-group schemes over $\mathbf{Z}[\zeta_{20}]$ are $\mathbf{Z}/2\mathbf{Z}$, μ_2 and $E[f]$.*

Proof. By the above discussion it suffices to show that all simple 2-group schemes have order 2. We apply [6, Prop.2.2] to the prime $p = 2$ and check "condition (A)". The root discriminant of the field L that appears in that proposition satisfies $\delta_L < 8 \cdot 5^{3/4} = 26.749\ldots$. Since this number is larger than the asymptotic value $4\pi e^{\gamma} \approx 22.3\ldots$ of Odlyzko's unconditional discriminant bound, we use his GRH bounds [4, 178–179]. These imply that $[L : \mathbf{Q}] < 600$. By the assumptions of [6, Prop.2.2], We have the following inclusions of fields

$$\mathbf{Q} \underset{16}{\subset} F(i) \underset{2\times 2\times 2}{\subset} K \underset{\leq 4}{\subset} L.$$

Here $K = \mathbf{Q}(\zeta_{40}, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \sqrt{\varepsilon_3})$ where the ε_i are a basis for the unit group of O_F modulo torsion. Let $\Gamma = \mathrm{Gal}(L/\mathbf{Q})$. The field $F(i) = \mathbf{Q}(\zeta_{40})$ is the largest abelian extension of $\mathbf{Q}$ inside L. By [9, Thm.11.1] the class number of $\mathbf{Q}(\zeta_{40})$ is 1. In addition, the unit $1 - \zeta_{40}$ generates the multiplicative group of the residue field $\mathbf{F}_{16}$ of the unique prime over 2. Therefore, by class field theory, the field $\mathbf{Q}(\zeta_{40})$ admits no abelian odd degree extension inside L. This implies that Γ'/Γ'' is a 2-group. By [6, Prop.3.2] we then see that Γ'' and hence $\mathrm{Gal}(L/F)$ are 2-groups.

It follows from [6, Prop.2.2] that all simple 2-group schemes over O_F have order 2 as required.

The next theorem describes various extensions of the three group schemes of order 2 by one another.

Theorem 2.2. *Over the ring O_F we have that*

(i) Any extension of constant 2-group schemes is constant; any extension of diagonalizable 2-group schemes is diagonalizable;

(ii) $\mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z}) = 0$*;*

(iii) the groups $\mathrm{Ext}^1_{O_F}(E[f], \mathbf{Z}/2\mathbf{Z})$ *and* $\mathrm{Ext}^1_{O_F}(\mu_2, E[f])$ *are zero;*

(iv) the group $\mathrm{Ext}^1_{O_F}(E[f], E[f])$ *has order 2; its non-trivial element is represented by the group scheme $E[2]$ of 2-torsion points of the elliptic curve E.*

Proof. By [6, Prop.2.6], parts *(i)* and *(ii)* follow from the facts that the class number of O_F is 1 and that there lies only one prime over 2 in O_F. To prove *(iii)*, consider an extension

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow E[f] \longrightarrow 0$$

over O_F. Since $E[f]$ is local, the extension is split over the completion $\widehat{O}_F$ at the prime $\pi = 1 + i$. Therefore G is killed by 2. The quadratic character that gives the Galois action is everywhere unramified and hence trivial. It follows that G is locally and generically trivial. Since there lies only one prime over 2, the Mayer-Vietoris sequence [6, Cor.2.4] then implies that G is split over O_F. This proves *(iii)*.

To prove *(iv)* consider an extension

$$0 \longrightarrow E[f] \longrightarrow G \longrightarrow E[f] \longrightarrow 0$$

over O_F. We use local results of Cornelius Greither's [3]. For $n \geq 0$ let U_n denote the multiplicative group $\{\varepsilon \in \widehat{O}_F^* : \varepsilon \equiv 1 \pmod{\pi^n}\}$. By Greither's theorem, $\mathrm{Ext}^1_{\widehat{O}_F}(E[f], E[f]) \cong U_3/U_2^2 = U_3/(U_3 \cap (\widehat{O}_F^*)^2)$. Moreover, it follows from the arguments in [3] that the points of the extension G corresponding to a unit $\varepsilon \in U_3$, generate the field $\mathbf{Q}_2(\zeta_{20}, \sqrt{\varepsilon})$. This implies that G is determined by its Galois module.

Since $\pm\varepsilon \equiv 1 \pmod{\pi^2}$, it follows that the number field generated by the points of G has conductor at most π^2 over F. The ray class field of F of conductor π^2 has degree 2. This follows from the fact that the global units 1 and $(1 - \zeta_{20}^a)^{15}$ generate a subgroup of $(1 + (\pi))/(1 + (\pi^2)) \cong \mathbf{F}_{16}$ of index 2. Therefore the Galois action on the points of G is either trivial or is given by the unique character of conductor (2). If it is trivial, the action is also locally trivial and hence G is trivial over $\widehat{O}_F$. By the equivalence of categories of [6, Prop.2.3], the extension G is then trivial. If the Galois action is not trivial, then locally it is also non-trivial. This follows from the fact that the class number of O_F is 1. This fixes the structure of G over $\widehat{O}_F$ and hence, by [6, Prop.2.3], there is only one choice for G. The exact sequence

$$0 \longrightarrow E[f] \longrightarrow E[2] \longrightarrow E[f] \longrightarrow 0$$

is non-split since the 2-torsion points of E generate the quadratic extension $F(\sqrt{\eta})$ of F. Here η denotes the unit $(1 + \sqrt{5})/2 \in O_F^*$. Therefore $E[2]$ provides the non-trivial class in $\mathrm{Ext}^1_{O_F}(E[f], E[f])$.

This proves the Theorem

3. 2-divisible groups over $\mathbf{Z}[\zeta_{20}]$.

In this section we prove Theorem 1.1. For any abelian variety A over $F = \mathbf{Q}(\zeta_{20})$ with good reduction everywhere, the group scheme $A[2^n]$ is a 2-group scheme over $O_F = \mathbf{Z}[\zeta_{20}]$.

Proposition 3.1. *Let A be an abelian variety over F with good reduction everywhere. Then the 2-group scheme $A[2^n]$ admits for each $n \geq 1$, a filtration with subquotients isomorphic to the group scheme $E[f]$.*

Proof. First consider the 2-torsion subgroup scheme $A[2]$ over O_F. It admits a filtration with simple subquotients. By Theorem 2.1 the simple subquotients of this filtration are isomorphic to $\mathbf{Z}/2\mathbf{Z}$, μ_2 or $E[f]$. By Theorem 2.2 *(ii)* and *(iii)* we can modify the filtration and obtain closed flat subgroup schemes G_1 and G_2 of $A[2]$ for which

$$0 \quad \hookrightarrow \quad G_1 \quad \hookrightarrow \quad G_2 \quad \hookrightarrow \quad A[2], \qquad (*)$$

and where G_1 is filtered with group schemes isomorphic to μ_2, the quotient G_1/G_2 is filtered with group schemes isomorphic to $E[f]$ and $A[2]/G_2$ is filtered with group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$. Let 2^a and 2^b denote the orders of G_1 and $A[2]/G_2$ respectively.

Next consider the group scheme $A[2^n]$. We filter it with its closed subgroup schemes $A[2^i]$ for $i = 1, \ldots, m$. All subquotients in this filtration are isomorphic to $A[2]$ and we filter these as in (*). By Theorem 2.2 *(ii)* and *(iii)* we can modify this filtration and obtain closed flat subgroup schemes H_1 and H_2 of $A[2^n]$ for which

$$0 \quad \hookrightarrow \quad H_1 \quad \hookrightarrow \quad H_2 \quad \hookrightarrow \quad A[2^n], \qquad (*)$$

and where H_1 is filtered with group schemes isomorphic to μ_2 and has order 2^{na}, where the quotient H_1/H_2 is filtered with group schemes isomorphic to $E[f]$ and where $A[2]/H_2$ is filtered with group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$ and has order 2^{nb}.

By Theorem 2.2 *(i)* the group scheme $A[2^n]/H_2$ is constant. It is a closed subgroup scheme of the abelian variety A/H_2. It follows from Weil's Riemann Hypothesis that the order 2^{bn} is bounded as $n \to \infty$. This is only possible when $b = 0$. Applying the same argument to the Cartier dual $H_1^\vee$ of H_1 and the abelian variety $A^{\mathrm{dual}}/H_1^\vee$ we see that $a = 0$ as well. It follows that $H_2 = A[2^n]$ and $H_1 = 0$ respectively.

This proves the Proposition.

Theorem 1.1 is now proved by an application of Proposition 3.2 below. The endomorphism ring $\mathrm{End}(\mathcal{E})$ of the 2-divisible group $\mathcal{E}$ of the elliptic curve E is isomorphic to the discrete valuation ring $\mathbf{Z}_2[i]$. Let f denote the prime element $1+i \in \mathrm{End}(\mathcal{E})$. The kernel of the morphsim $f : \mathcal{E} \longrightarrow \mathcal{E}$ is denoted by $\mathcal{E}[f]$. It is the group scheme $E[f]$ of order 2 that appears in section 2. By Proposition 3.1 the subgroup schemes $A[2^n]$ of an abelian variety A with good reduction everywhere over $\mathbf{Q}(\zeta_{20})$ is filtered by group schemes isomorphic to $\mathcal{E}[f]$. By Theorem 2.2 *(iv)* and the fact that the points of $E[2]$ are not defined over F, the condition of Proposition 3.2 below is satisfied. It follows that the 2-divisible group of A is isogenous to $\mathcal{E}^g$ for some $g \geq 0$. Faltings's Theorem [1] implies then that A and E^g are isogenous over F as required.

Proposition 3.2. *Let O be a Noetherian domain of characteristic 0 and let $\mathcal{G}$ be a p-divisible group over O. Suppose that $R = \mathrm{End}(\mathcal{G})$ is a discrete valuation ring with prime element f. Let $k = R/fR$. If the connecting homomorphism*

$$\mathrm{Hom}_O(\mathcal{G}[f], \mathcal{G}[f]) \quad \longrightarrow \quad \mathrm{Ext}^1_O(\mathcal{G}[f], \mathcal{G}[f])$$

associated to the exact sequence $0 \to \mathcal{G}[f] \to \mathcal{G}[f^2] \to \mathcal{G}[f] \to 0$ is an isomorphism of 1-dimensional k-vector spaces, then every p-divisible group over O that can be filtered with group schemes isomorphic to $\mathcal{G}[f]$, is isogenous to a power of $\mathcal{G}$.

Here a p-divisible group $\mathcal{H}$ is said to be filtered by $\mathcal{G}[f]$ if the group scheme $\mathcal{H}[p]$ of p-torsion points admits a filtration by closed flat subgroup schemes with successive subquotients isomorphic to $\mathcal{G}[f]$. The condition implies that all group schemes $\mathcal{H}[2^n]$ admit such filtrations. See [7] for a proof of Proposition 3.2.

Bibliography

[1] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983) 394–366.

[2] Fontaine, J.-M.: Il n'y a pas de variété abélienne sur **Z**, *Invent. Math.* **81**, (1985) 515–538.

[3] Greither, C.: Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring, *Math. Zeitschrift* **210** (1992) 37–67.

[4] Martinet, J.: Petits discriminants des corps de nombres, in J.V. Armitage, *Journées Arithmetiques 1980*, CUP Lecture Notes Series **56**, Cambridge University Press, Cambridge 1981.

[5] Schoof, R.: Abelian varieties over $\mathbf{Q}(\sqrt{6})$ with good reduction everywhere, in "Class Field Theory – Its Centenary and Prospect" (ed. by K. Miyake), Advanced Studies in Pure Mathematics, Tokyo 2001.

[6] Schoof, R.: Abelian varieties over cyclotomic fields with good reduction everywhere, submitted.

[7] Schoof, R.: Semi-stable abelian varieties over **Q**, preprint.

[8] Tate, J.T. and Oort, F.: Group schemes of prime order, *Ann. Scient. École Norm. Sup.* **3** (1970) 1–21.

[9] Washington, L.C.: *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York 1982.