MR488287 (80c:14015) 14G25 (10D05)
Mazur, B. [Mazur, Barry]
Modular curves and the Eisenstein ideal.
Inst. Hautes Études Sci. Publ. Math. *No. 47* (1977), 33–186 (1978).

The main subjects treated in this paper are: (i) classification of rational points of finite order (respectively, rational isogeny) of elliptic curves over a fixed number field K, and (ii) study of rational points of $X_0(N)$ and its Jacobian J, where $X_0(N)$ denotes the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$. As for the first problem (i), when K is $\mathbf{Q}$, there is a conjecture of A. Ogg which asserts that the group of $\mathbf{Q}$-rational points of an elliptic curve over $\mathbf{Q}$ is isomorphic to one of the following 15 groups: $\mathbf{Z}/m\mathbf{Z}$ ($m \leq 10$ or $m = 12$) or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\nu\mathbf{Z}$ ($\nu \leq 4$). The author verifies this conjecture by showing that there is no elliptic curve over $\mathbf{Q}$ which has $\mathbf{Q}$-rational points of order N when N is prime and $N = 11$ or $N \geq 17$. (Work of D. Kubert had reduced the problem to this case.) The proof is based on the fact labeled (III) below concerning rational points of J.

To describe the results on the second problem (ii), to which most of this paper is devoted, let N be a prime number and let n be the numerator of $(N-1)/12$. We hereafter assume that $n > 1$ (or equivalently, $N = 11$ or $N \geq 17$). It had been proved by Ogg that the divisor class of $(0) - (\infty)$ in J, where 0 and ∞ denote two cusps on $X_0(N)$, has order n. One of the main results on the structure of $J(\mathbf{Q})$ is: (I) the torsion part of $J(\mathbf{Q})$ is a cyclic group of order n generated by the class of $(0) - (\infty)$. In addition, the following result is obtained: (II) the "Shimura subgroup" is the maximal "μ-type" subgroup of J, where μ-type means that it is the Cartier dual of a constant group, and the Shimura subgroup is a μ-type cyclic subgroup of order n in J obtained from an étale covering of $X_0(N)$. To prove these results (both of which had been conjectured by Ogg) and to obtain more information about the rational points of J, the author introduces the "Eisenstein ideal" in the Hecke algebra. Namely, let $\mathbf{T}$ (the Hecke algebra) denote the $\mathbf{Z}$-algebra generated by the Hecke operators T_l (l prime, $\neq N$) and the involution w, which corresponds to $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$, acting on the space of cusp forms of weight 2 with respect to $\Gamma_0(N)$. By definition, the Eisenstein ideal $\mathfrak{J}$ of $\mathbf{T}$ is the ideal generated by $1 - T_l + l$ (l prime, $\neq N$) and $1 + w$. $\mathbf{T}$ naturally acts on J, and one can decompose it (up to $\mathbf{Q}$-isogeny, or equivalently $\mathbf{C}$-isogeny by a result of K. Ribet) according to the decomposition of Spec$(\mathbf{T})$ into its irreducible components. Let $\tilde{J}$ (the Eisenstein quotient of J) be the quotient by an abelian subvariety of J, whose simple factors correspond to the irreducible components of Spec$(\mathbf{T})$ which meet the support of $\mathfrak{J}$. Then it is true that: (III) the Mordell-Weil group $\tilde{J}(\mathbf{Q})$ is finite, and the natural map $J \to \tilde{J}$ induces an isomorphism of the torsion part of $J(\mathbf{Q})$ onto $\tilde{J}(\mathbf{Q})$. From this, one easily obtains: (IV) the group of $\mathbf{Q}$-rational points of $X_0(N)$ is finite (for N as above). Next, let $J_+ = (1+w)J$, and let J^- be the quotient of J by J_+. Then it is proved that $J \to \tilde{J}$ factors through $J \to J^-$, and (V) the Mordell-Weil group $J_+(\mathbf{Q})$ is torsion free and of positive rank if $\dim J_+ \geq 1$ (the latter assertion being in accord with the conjecture of Birch and Swinnerton-Dyer).

To obtain these results, one needs a detailed study of the algebra $\mathbf{T}$ and the division points of J

by ideals of $\mathbf{T}$, especially by $\mathfrak{J}$ and the prime ideals containing $\mathfrak{J}$. This is done in Chapter II of this paper. The main tools are the theory of (quasi-) finite flat group schemes over $\mathbf{Z}$ (Chapter I), and the theory of modular forms over rings (the first part of Chapter II). The above results (I)-(V) (and others) are then established in Chapter III. Also in the final two sections, some relevant results in connection with the earlier works of the author are obtained. For a more detailed survey of the content of this paper, the reader is referred to the paper by the author and J.-P. Serre [Séminaire Bourbaki (1974/1975), Exp. No. 469, pp. 238–255, Lecture Notes in Math., Vol. 514, Springer, Berlin, 1976; MR0485882 (58 #5681)]. We note finally that the problem (ii) concerning the $\mathbf{Q}$-rational isogeny (of prime degree) has been solved by the author in a subsequent paper [Invent. Math. **44** (1978), no. 2, 129–162].

Reviewed by *M. Ohta*