MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 131
JULY 1975, PAGES 951–964

Elliptic Curves Over Finite Fields. II

By I. Borosh, C. J. Moreno and H. Porta

Abstract. The class groups of certain elliptic function fields without complex multiplications are computed. Questions about the structure of these groups and the arithmetical nature of their orders are considered.

1. Introduction. The present work gives in greater detail the computations outlined in the Boulder paper [2]. Let E be an elliptic curve whose Néron minimal model is

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbf{Z}$ and of conductor N. For a fixed prime p, the same equation for E with coefficients read in the finite field $\mathbf{F}_p$ of p elements defines an elliptic curve $E(\mathbf{F}_p)$ over the algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$ for all primes p not dividing the conductor N. In this paper we study that part of $E(\overline{\mathbf{F}}_p)$ which is left fixed by the action of the Galois group $G = \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$. More precisely, we study the structure of the finite abelian group,

$$E(\mathbf{F}_p): y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \mod(p),$$

consisting of the points on the elliptic curve E whose coordinates lie in the finite field $\mathbf{F}_p$ and also the point at infinity. We will not consider the somewhat simpler question of the structure of $E(\mathbf{F}_p)$ for those primes p which divide the conductor of E, since this can be done mechanically once the Kodaira type of the reduced fiber is known.

The starting point of our investigations was the important work of Shimura [11] where knowledge of the number of points on the curve,

$$E(\mathbf{F}_p): y^2 \equiv 4x^3 - \left(\frac{4 \cdot 31}{3}\right)x - \left(\frac{41 \cdot 61}{27}\right) \mod(p),$$

was used to obtain information about the nonsolvable field extensions obtained by adjoining to the rationals the coordinates of the l-division points on the curve,

$$y^2 = 4x^3 - \left(\frac{4 \cdot 31}{3}\right)x - \left(\frac{41 \cdot 61}{27}\right),$$

which as Tate has observed is isogenous to $y^2 - y = x^3 - x^2$. The computations given by Shimura in [11] for

$$N_p = \mathrm{Card}\, E(\mathbf{F}_p) = p - a_p + 1$$

Received February 11, 1974; revised April 29, 1974.
AMS (MOS) subject classifications (1970). Primary 14G15; Secondary 10D99.
Key words and phrases. Elliptic curves, modular forms, finite fields, traces of Frobenius.

were obtained by computing the coefficients a_n in the infinite product,

$$f(z) = q \prod_{n=1}^{\infty} (1 - q^n)^2(1 - q^{11n})^2 = \sum_{n=1}^{\infty} a_n q^n, \qquad q = \exp(2\pi iz),$$

which is a cusp form of weight 2 associated with the Hecke congruence subgroup $\Gamma_0(11)$. The traces of Frobenius a_p in Shimura [11] are given for primes $p \leqslant 2000$. D. H. Lehmer also computed the a_p using the above product expansion for all primes $p \leqslant 30000$; incidentally, Lehmer found many primes p for which $a_p = 0$.

There are in nature eleven other curves like the one considered by Shimura which are uniformized by modular forms on $\Gamma_0(N)$. Affine models for these have been given by Birch [1]. Thus in principle one can compute Card $E(\mathbf{F}_p)$ in essentially two different ways: namely, by counting the number of points on the Birch models (unfortunately, these are not given in Néron minimal form!) and by computing the traces of Frobenius via an explicit construction of the cusp form associated with the modular curve which can be obtained as a linear combination of suitable theta functions.

For $N = 14$ Birch [1] has given the model,

$$E_{14}\colon y^2 + xy = x^3 + 3x^2 + 8x.$$

The associated cusp form of weight 2 and level 14 as given by Doi and Naganuma [7] is

$$\sum_{n=1}^{\infty} a_n q^n = q \prod_{n=1}^{\infty} (1 - q^n)(1 - q^{2n})(1 - q^{7n})(1 - q^{14n}).$$

In [10] Serre has given an affine model of a curve of conductor 14,

$$E_s\colon y^2 + xy + y = x^3 - x.$$

Our preliminary computations gave that the traces of Frobenius for primes $p \leqslant 5000$ were identical for both curves E_{14} and E_s. Also, for all primes $p \leqslant 2000$ we computed the groups $E_{14}(\mathbf{F}_p)$ and $E_s(\mathbf{F}_p)$ and found that they agree except for the splitting of the 3-primary component. This suggested strongly the existence of an isogeny of degree 3. That this is in fact true can be explained by observing that the elliptic curve E_s is in fact the curve $X_1(14)$ in the notation of Ogg [9], $E_{14} = X_0(14)$, and $X_1(14)$ covers $X_0(14)$ by an isogeny of degree 3. More explicitly, E_s is equivalent to $y^2 + xy - y = x^3$; and dividing out by the cyclic group of order 3 generated by (0, 0), we get $y^2 + xy = x^3 + 3x^2 + 8x$ which is Birch's equation. We might add that the general rule for dividing $y^2 + a_1xy + a_3y = x^3$ by the point (0, 0) is $y^2 + a_1xy + 3a_3y - 6a_1a_3x + a_1^2a_3 - 9a_3^2$.

The contents of the paper are as follows. In Section 2 we give a brief description of the group law on $E(\mathbf{F}_p)$ which is useful in computation. In Section 3 we describe a method for computing the primary decomposition of $E(\mathbf{F}_p)$ by machine. In Section 4 we present the numerical results obtained. In this same section we also give various conjectures and theorems which were suggested by the machine computations. The primary decomposition of $E(\mathbf{F}_p)$ for various curves and primes $p \leqslant 5000$ and also for some other primes $p \leqslant 5000$ are given at the end of the paper.

The present version of the paper owes much to the suggestions of many people.

Here we would like to record our thanks to the referee, who among other things pointed out the isogeny between E_{14} and E_s given above and also suggested the first and third remarks which appear at the end of Section 3.

2. The Group Law. When the elliptic curve E is given in Weierstrass normal form,

$$E\colon y^2 = 4x^3 - g_2x - g_3,$$

with $g_2, g_3 \in \mathbf{Z}$, the group law for E in characteristic zero corresponds simply to the addition formulas for the Weierstrass p-function,

$$p(z) = z^{-2} + \sum_{\omega\in\Omega}{}' ((z-\omega)^{-2} - \omega^{-2}).$$

Now if the elliptic curve E has good reduction at a prime p, the formula for the group law of E can be reduced modulo p to give the group law for $E(\mathbf{F}_p)$. This procedure works for almost all primes not dividing the conductor. To obtain formulas defining the group law for $E(\mathbf{F}_p)$ which work for all primes not dividing the conductor one must work with the Néron minimal model of E and obtain explicit formulas in characteristic zero and then read them modulo the prime p to obtain the group law for $E(\mathbf{F}_p)$.

In characteristic zero the group law is obtained by the tangent-chord process of Euler: "Three collinear points on E add up to zero," where the zero element on E is taken to be the point of infinity $P_\infty = (\infty, \infty)$. Thus, if $P_1 = (z_1, y_1)$ and $P_2 = (x_2, y_2)$ are two distinct points on E, their sum $P_3 = (x_3, y_3)$ is the inverse of the point $-P_3 = (x_3^*, y_3^*)$ where the curve E intersects the line passing through the points P_1 and P_2. To obtain P_3 from $-P_3$ one considers a line passing through $-P_3, P_3$, and P_∞. For an elliptic curve with affine model,

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

the coordinates of $P_3 = (x_3, y_3)$ are given by

$$x_3 = -x_1 - x_2 + m^2 + a_1m - a_2, \qquad y_3 = -y_1 - mx_3 + x_1m - a_1x_3 - a_3,$$

where $m = (y_2 - y_1)/(x_2 - x_1)$. The double of a point, i.e. the case $P_1 = P_2$, is found similarly by first observing that the tangent to E at P_1 has a contact of second order (the intersection multiplicity is 2) and then finding the other point of intersection. The coordinates of $2P_1 = P = (x, y)$ are

$$x = -2x_1 + m^2 + a_1m - a_2, \qquad y = -a_1x - a_3 - y_1 - m(x - x_1),$$

where

$$m = (3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)/(2y_1 + a_1x_1 + a_3).$$

The group law for $E(\mathbf{F}_p)$ is now given by the above formulas read modulo p. The good reduction of the elliptic curve E at a prime p which does not divide the conductor of E guarantees that the group law for $E(\mathbf{F}_p)$ given by the above formulas are well defined modulo p.

The l-division equation plays a very important role in the following considerations. If $t = (x(t), y(t))$ is a point on the elliptic curve, then the lth multiple lt of the point t

has coordinates $lt = (x(lt), y(lt))$, where

$$x(lt) = B_l(x)/A_l(x)^2 \quad \text{and} \quad y(lt) = yD_l(x)/A_l(x)^3.$$

The polynomial $A_l(x)$ is of degree $(l^2 - 1)/2$ and is classically known as the l-division equation. For small l it can be computed by iterating the group law. For more details see the expository article by Cassels [5].

3. Machine Computations.

3.1. *Computation of the Points and the Order of the Group.* Let

$$E(\mathrm{F}_p)\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be the reduction mod p of the Néron minimal model for E. To compute the points on $E(\mathrm{F}_p)$, we take a ξ in F_p and solve for y the quadratic equation,

$$y^2 + (a_1\xi + a_3)y + (-\xi^3 - a_2\xi^2 + a_4\xi + a_6) = 0,$$

using the formal expression $y = (-a_1\xi - a_3 \pm \Delta^{1/2})/2$, where

$$\Delta = (a_1\xi + a_3)^2 + 4(\xi^3 + a_2\xi^2 + a_4\xi + a_6).$$

This process yields two points on the curve, one point, or no point depending on whether Δ is a nonzero square in F_p, zero or a nonsquare. The repeated use of this algorithm for all $\xi = \mathrm{F}_p$ gives all the points on $E(\mathrm{F}_p)$ except the point of infinity $P_\infty = (\infty, \infty)$. The computation of the square roots in the above formula was done by squaring the numbers $1, 2, \ldots, (p - 1)/2$ and storing them for use for all points of the curve. The above method gives immediately the number of points on $E(\mathrm{F}_p)$:

$$N_p = p - a_p + 1$$

and hence the value of a_p. This is obtained by $O(p)$ operations.

3.2. *The Primary Decomposition of the Group.* We obtain first the prime decomposition of N_p. The actual determination of the structure of the l-primary component is done as follows. If there are $l - 1$ points of order l in $E(\mathrm{F}_p)$, then the l-primary component is cyclic. Otherwise the l-primary component has rank 2, and the problem now becomes that of determining how the l-primary component breaks as a direct sum of two cyclic groups. Now if the rank of the l-primary part of $E(\mathrm{F}_p)$ is 2 and $l^2 \| N_p$ or $l^3 \| N_p$, then

$${}_lE(\mathrm{F}_p) = (Z/lZ) \oplus (Z/lZ) \quad \text{or} \quad {}_lE(\mathrm{F}_p) = (Z/l^2Z) \oplus (Z/lZ),$$

respectively. If the rank is 2 and $l^m \| N_p$ with $m \geqslant 4$, then let m_i be the number of points of order l^i for $i = 1, 2, \ldots, [m/2]$. Let j be the largest i such that $m_i = l^{2i} - l^{2i-2}$, then the l-primary component of $E(\mathrm{F}_p)$ is

$${}_lE(\mathrm{F}_p) = (Z/l^jZ) \oplus (Z/l^{m-j}Z).$$

Remarks. (1) An important fact used implicitly in the computation of $E(\mathrm{F}_p)$ is that the kernel ${}_mE$ of multiplication by m in the elliptic curve $E(\overline{\mathrm{F}}_p)$ is a product of two cyclic groups of order m and carries a natural symplectic structure. Thus if all the m^2 points of ${}_mE$ have coordinates in the field F_p, then F_p contains all mth root of unity, i.e. $m|(p - 1)$. This gives immediately the fact that if N_p and $p - 1$ are relatively prime, then $E(\mathrm{F}_p)$ is cyclic, or equivalently if $a_p - 2$ and $p - 1$ are relatively prime, then $E(F_p)$ is cyclic. This criterion greatly simplifies the computations since the size of $a_p - 2$ is $O(p^{1/2})$ by the "Riemann Hypothesis".

(2) We do not have to compute the order of all the points of $E(F_p)$ in order to determine the group structure. If $l^i \| N_p$, we only need to know at most the number of points of order not larger than l^j, $(j = [i/2])$; this simply means that we have to iterate the group operation for all the points of $E(F_p)$ at most $l^j - 1$, $(j = [i/2])$, times. The number of operations involved for every point is $O(l^j) = O(p^{1/2})$, and since $N_p = p - a_p + 1 = O(p)$, we get that the total number of operations involved in computing the group structure of $E(F_p)$ is at most $O(p^{3/2})$.

(3) When two elliptic curves E_1 and E_2 are connected by an isogeny of degree d, the two groups $E_1(F_p)$ and $E_2(F_p)$ are the same except for the l-component for each prime $l|d$. As an example, we consider the case of the two elliptic curves

$$E_1\colon y^2 - y = x^3 - x^2 \quad \text{and} \quad E_2\colon y^2 + y = x^3 - x^2 - 10x - 20.$$

These are the curves $X_1(11)$ and $X_0(11)$, respectively, in the notation of Ogg [9] which in fact are connected by an isogeny of degree 5. This leads to the following observations:

(i) The groups $E_1(F_p)$ and $E_2(F_p)$ are the same, except for the 5-component.

(ii) If $p \not\equiv$ mod (5), then the 5-component of both is cyclic and so the two groups are the same.

(iii) Using Kummer Theory, Ogg [9] shows that all 25 points on E_2 of order dividing 5 are rational over the cyclotomic field $Q(e^{2\pi i/5})$, and for $p \equiv 1 \mod (5)$ the group $E_2(F_p)$ is not cyclic.

In Table 2 we have given the structure of $E_1(F_p)$ from which we can easily compute the group $E_2(F_p)$ using the remarks above.

Notation. In the subsequent tables the primary decomposition of a group will be written for simplicity in the form $(m_1, m_2m, \ldots, m_k)$ which stands for

$$(Z/m_1Z) \oplus (Z/m_2Z) \oplus \cdots \oplus (Z/m_kZ).$$

4. Numerical Results.

4.1. Computations were carried out for six elliptic curves whose equations, j invariants, conductors N and discriminants Δ are given below. These curves were taken from Serre's article [10] where the Galois properties of their fields of l-division points are studied:

TABLE A

Elliptic curve	*Equation*	*j-invariant*	*Conductor*	*Discriminant*
E_1	$y^2 - y = x^3 - x^2$	$-2^{12}/11$	11	-11
E_2	$y^2 + y = x^3 - x^2 - 10x - 20$	$-2^{12} \cdot 31^3/11^5$	11	-11^5
E_3	$y^2 + xy = x^3 + x^2 - 2x - 7$	-11^2	11^2	-11^4
E_4	$y^2 + y = x^3 + x^2$	$-2^{12}/43$	43	-43
E_5	$y^2 + xy + y = x^3 - x$	$-5^6/2^2 \cdot 7$	$2 \cdot 7$	$-2^2 \cdot 7$
E_6	$y^2 + y = x^3 - x$	$2^{13} \cdot 3^3/37$	37	37

The original computations were carried out for primes in the range from 2 to

5000. Table 1 records the traces of the Frobenius endomorphism a_p for the above curves for primes in the range 2 to 2000. The results we obtained for E_1 were compared with those given by Shimura in [11] and are not included here. Curves E_1 and E_2 are isogenous and thus have the same a_p (Vélu [12]).

Tables 2, 3, 4 and 5 give the prime p and the primary decomposition (notation: PD) of $E(\mathbf{F}_p)$; the order $N_p = \text{Card } E(\mathbf{F}_p)$ can easily be computed from this data. In Table 2 the results for E_1 are presented and from these we can easily compute $E_2(\mathbf{F}_p)$ using the remarks at the end of Section 3. Each table goes up to 500 and presents some additional primes.

As is well known, the curve E_1 has a rational point of order 5 and hence $5|N_p$ for all $p \neq 11$. Similarly E_5 has a rational point of order 6 and hence $6|N_p$ except for $p = 2$ and $p = 7$.

The computations suggest that the reduction of the same curve for various primes p may lead to the same order N_p but to nonisomorphic groups. Below we give several examples:

TABLE B

Curve	*Prime*	N_p	$E(\mathbf{F}_p)$	*Curve*	*Prime*	N_p	$E(\mathbf{F}_p)$
E_1	557	560	(16, 5, 7)	E_4	719	712	(2, 4, 89)
E_1	599	560	(2, 8, 5, 7)	E_4	727	712	(8, 89)
E_2	1021	1000	(2, 4, 5, 25)	E_5	1579	1620	(2, 2, 3, 27, 5)
E_2	1031	1000	(8, 5, 25)	E_5	1667	1620	(2, 2, 81, 5)
E_2	967	1000	(8, 125)	E_6	1301	1372	(8, 3, 53)
E_3	4091	4180	(4, 5, 11, 19)	E_6	1307	1372	(2, 4, 3, 53)
E_3	4201	4180	(2, 2, 5, 11, 19)				

Other examples may be found in the tables below.

An interesting observation that was made for the curve E_1 of conductor 11 and E_3 of conductor 11^2 is that $3|\text{Card } E_1(\mathbf{F}_p)$ if and only if $3|\text{Card } E_3(\mathbf{F}_p)$. Also, the 3-primary component of $E_1(\mathbf{F}_p)$ splits if and only if the 3-primary component of $E_3(\mathbf{F}_p)$ splits. These observations can be checked in Tables 2 and 3. Below we give examples of the simultaneous splitting.

TABLE C

P	N_p	$E_1(\mathbf{F}_p)$	N_p	$E_3(\mathbf{F}_p)$
337	360	(8, 3, 3, 5)	351	(3, 9, 13)
523	540	(4, 3, 9, 5)	540	(4, 3, 9, 5)
1087	1080	(2, 4, 3, 9, 5)	1134	(2, 3, 27, 7)
2437	2520	(8, 3, 3, 5, 7)	2520	(2, 4, 3, 3, 5, 7)
2719	2790	(2, 3, 3, 5, 31)	2664	(8, 3, 3, 37)
2749	2700	(4, 3, 9, 25)	2673	(3, 81, 11)
3331	3375	(3, 9, 5, 25)	3312	(16, 3, 3, 23)
3469	3555	(3, 3, 5, 79)	3429	(3, 9, 127)
3709	3690	(2, 3, 3, 5, 41)	3753	(3, 9, 139)
4003	4050	(2, 3, 27, 25)	3960	(8, 3, 3, 5, 11)
4483	4590	(2, 3, 9, 5, 17)	4500	(4, 3, 3, 125)
4801	4725	(3, 9, 5, 5, 7)	4779	(3, 27, 59)

The above are all the examples that appear in the range up to 4963.

TABLE 1. *Traces of Frobenius*

P	E_1, E_2	E_3	E_4	E_5	E_6
2	-2	1	-2	*	-2
3	-1	2	-2	-2	-3
5	1	1	-4	0	-2
7	-2	-2	0	*	-1
11	*	*	3	0	-5
13	4	1	-5	-4	-2
17	-2	-5	-3	6	0
19	0	6	-2	2	0
23	-1	2	-1	0	2
29	0	9	-6	-6	6
31	7	-2	-1	-4	-4
37	3	-3	0	2	*
41	-8	-5	5	6	-9
43	-6	0	*	8	2
47	8	2	4	-12	-9
53	-6	9	-5	6	1
59	5	8	-12	-6	8
61	12	6	2	8	-8
67	-7	2	-3	-4	8
71	-3	12	2	0	9
73	4	-2	2	2	-1
79	-10	-10	-8	8	4
83	-6	6	15	-6	-15
89	15	-9	-4	-6	4
97	-7	-13	7	-10	4
101	2	-10	-9	0	3
103	-16	8	1	-4	18
107	18	6	-12	12	-12
109	10	-11	7	2	-16
113	9	-9	-20	6	-18
127	8	-16	1	-16	1
131	-18	0	8	18	-12
137	-7	-10	6	18	-6
139	10	-2	19	14	4
149	-10	17	12	-18	-5
151	2	-16	-20	8	16
157	-7	2	-10	-4	23
163	4	-2	14	-16	-18
167	-12	12	-9	-12	-12
173	-6	6	6	-12	9
179	-15	24	20	-12	18
181	7	1	10	20	5
191	17	8	-16	24	-4
193	4	-5	3	14	-26
197	-2	-11	2	-18	3
199	0	24	14	20	2
211	12	12	2	-4	-13
223	19	-20	-28	8	-17
227	18	-24	-4	18	-16
229	15	9	-15	-4	7
233	24	-21	6	-6	6
239	-30	6	16	24	-6
241	-8	22	-12	-10	14
251	-23	-2	-23	-18	-2
257	-2	19	-24	18	0
263	14	-22	-18	0	19
269	10	1	-25	-12	-6
271	-28	20	23	-16	-31
277	-2	1	-32	-10	12
281	-18	6	19	-6	12
283	4	28	21	-22	4
293	24	9	-26	24	-2
307	8	-22	-7	2	-17
311	12	24	15	-24	0
313	-1	23	22	-10	22
317	13	-2	9	6	22
331	7	-20	-26	8	-2
337	-22	-13	-3	14	-25
347	28	28	28	-24	-10
349	30	-27	14	-28	6
353	-21	-9	-31	18	8
359	-20	-2	19	-24	-15
367	-17	-14	-32	8	8
373	-26	22	32	14	-19
379	-5	-32	11	-16	15
383	-1	20	32	36	20
389	-15	-3	6	18	4
397	-2	13	-6	20	-5
401	2	23	5	-18	18
409	-30	-21	-24	14	20
419	20	2	-28	6	7
421	22	13	-10	-10	-24
431	-18	12	-21	24	-30
433	-11	19	-12	-34	9
439	40	22	17	8	28
443	-11	-20	-4	-12	1
449	35	-13	30	18	36
457	-12	39	-18	-10	18
461	12	33	30	12	30
463	-11	-20	4	32	-22
467	-27	12	6	-6	-2
479	20	-16	21	-36	14
487	23	2	36	-16	-24
491	-8	-2	-6	-12	-28
499	20	8	-8	-4	12
503	-26	-33	6	0	16
509	15	-42	-15	36	-31
521	-3	30	14	6	-33
523	-16	-16	12	2	-22
541	-8	34	1	38	20
547	8	-16	-29	8	8
557	-2	-2	-3	6	-18
563	4	34	37	30	-30
569	0	6	7	6	-24
571	-23	-22	-14	32	7
577	33	-21	-20	2	0
587	28	-14	2	-42	-32
593	44	11	-16	-6	-5
599	40	34	-1	-24	1
601	2	-13	-4	26	-22
607	-22	-10	-4	32	-32
613	-16	17	-18	2	15
617	18	-9	-21	6	17
619	-25	2	36	26	-1
631	7	-14	-6	-16	-28
641	-33	-9	12	-18	-1
643	29	-10	-36	14	14
647	-7	20	-12	-12	-8
653	-41	-14	-14	18	-24
659	10	22	-19	-24	-15
661	37	13	31	-40	-28
673	14	-10	14	26	27
677	-42	-27	34	-12	-11
683	-16	2	-9	-12	18
691	17	20	-40	-46	-20
701	2	17	-2	18	-12
709	-25	-10	-1	-46	40
719	15	30	8	12	39
727	3	-42	16	44	16
733	-36	9	32	-40	7
739	50	-10	-10	-16	-9
743	4	-38	-24	24	21
751	-23	-20	-6	-40	25
757	-22	53	28	2	-50
761	12	-21	20	-18	-35
769	20	11	-42	14	26
773	-6	-42	-4	24	-9
787	-32	28	4	-22	-5
797	53	-10	-42	-12	52
809	0	6	26	6	2
811	-38	28	-14	2	47
821	22	-2	49	6	-47
823	39	-24	-1	-40	-16
827	-52	-10	-36	-36	22
829	25	-47	44	56	-4
839	-5	46	-40	12	44
853	14	17	-29	44	26
857	8	-22	-10	-18	-48

TABLE 1 (*Continued*)

P	E_1, E_2	E_3	E_4	E_5	E_6
859	-15	24	-32	14	-20
863	24	-54	-6	-24	-24
877	-12	-27	41	-22	50
881	-43	35	37	-54	-14
883	4	-20	31	20	48
887	-22	-46	-22	-36	25
907	-12	12	47	44	52
911	12	-24	-22	48	26
919	10	28	-49	56	-58
929	-30	-21	-6	6	18
937	8	23	32	2	37
941	42	-27	33	-24	-10
947	-27	-42	-33	24	12
953	34	31	22	-54	61
967	-32	22	37	32	-14
971	47	2	-13	-6	-8
977	-27	-57	34	-6	28
983	39	-36	-24	-36	9
991	-8	-20	2	-16	-18
997	38	53	4	8	-42
1009	-10	-49	-18	-34	-47
1013	39	-42	-22	-36	36
1019	-10	-46	-30	36	46
1021	22	-2	-14	-4	-62
1031	32	50	46	0	-4
1033	-16	11	13	26	3
1039	5	-10	34	-4	-59
1049	-55	-25	6	-30	-4
1051	2	-16	-60	44	-16
1061	-13	-43	-40	-30	-62
1063	44	20	12	-16	7
1069	-20	1	32	8	-30
1087	8	-46	20	8	12
1091	-58	-10	40	30	30
1093	-51	30	-46	-22	-36
1097	-42	39	12	-6	36
1103	-51	24	54	48	-8
1109	-30	42	0	36	-35
1117	48	-27	4	-34	33
1123	24	24	60	-46	-22
1129	50	-13	-26	50	50
1151	2	-46	-30	-12	-25
1153	-31	-46	21	2	18
1163	34	-38	32	-60	-36
1171	-3	12	-52	20	-22
1181	-18	-3	-40	60	57
1187	-12	66	-48	-12	-33
1193	-21	-21	32	66	-11
1201	2	23	-55	14	44
1213	-41	46	-59	26	-12
1217	-42	-57	-30	-6	-41
1223	14	56	-6	-24	30
1229	60	6	3	30	-48
1231	-18	0	-26	-28	-19
1237	18	45	-20	-40	-42
1249	40	-5	-50	26	-13
1259	-25	56	-12	18	8
1277	-47	46	-20	24	-24
1279	-15	24	20	20	64
1283	-36	42	-37	0	-36
1289	0	-21	2	30	48
1291	-8	-14	-9	-58	35
1297	48	-33	-38	-34	-38
1301	27	57	39	-48	30
1303	39	12	39	8	56
1307	28	-2	-27	42	36
1319	-30	-66	-18	-24	-4
1321	47	35	7	62	35
1327	68	-46	66	32	-2
1361	12	6	0	-18	66
1367	-72	-42	-12	-24	62
1373	39	9	-45	-30	-2
1381	-68	61	52	-22	63
1399	60	-54	32	-40	-25
1409	-15	-9	42	18	-1
1423	29	-58	29	56	-34
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
1433	54	-9	-35	42	-54
1439	0	42	-42	24	-53
1447	28	-38	22	-64	-57
1451	52	22	-50	-48	22
1453	-71	13	-10	50	47
1459	-20	64	-23	38	-37
1471	22	28	-1	32	-1
1481	32	-13	52	-6	13
1483	49	64	19	-46	-39
1487	58	34	24	0	-3
1489	-15	30	40	-58	-22
1493	-36	-27	21	30	6
1499	55	-20	26	-12	-66
1511	37	52	41	0	-30
1523	-41	34	60	-72	-8
1531	32	56	0	2	16
1543	-36	24	-56	32	-1
1549	-15	9	14	-34	-14
1553	-56	34	12	42	14
1559	-60	6	-44	-12	-42
1567	-52	-10	32	-16	14
1571	-28	20	33	66	12
1579	-30	6	-19	-40	31
1583	34	-14	9	0	-44
1597	-32	34	-74	-58	28
1601	2	-49	13	66	-46
1607	33	24	37	48	72
1609	-10	35	14	26	-4
1613	-6	9	-80	-72	-54
1619	-20	-32	-36	-60	-33
1621	22	-47	36	74	17
1627	78	0	47	-10	-44
1637	33	9	-56	0	53
1657	-2	-2	1	-34	-26
1663	4	34	-26	8	8
1667	48	6	24	48	-52
1669	50	17	-14	32	54
1693	-6	66	-26	56	-62
1697	-42	-9	-18	-42	72
1699	40	34	50	-10	65
1709	-45	30	-50	54	-3
1721	-3	78	-45	-6	-40
1723	-46	-46	58	-4	-5
1733	-6	6	45	-6	44
1741	17	-31	-59	-76	68
1747	-57	-24	-52	56	28
1753	34	19	4	-46	10
1759	-40	-22	28	32	22
1777	8	-82	-62	50	-62
1783	59	-64	34	-16	36
1787	-57	12	-65	72	-4
1789	10	-35	78	-10	-16
1801	52	-38	73	-34	3
1811	12	42	-26	42	34
1823	-56	28	-35	-24	-9
1831	-43	-76	-8	-40	-78
1847	-52	-22	29	12	12
1861	62	-43	-16	8	81
1867	28	-38	14	50	2
1871	-3	-42	72	48	-17
1873	-6	-42	-55	2	26
1877	18	42	16	78	22
1879	-35	-2	54	44	-70
1889	70	-5	-45	18	66
1901	77	-79	3	-18	-60
1907	-52	-58	-53	42	-58
1913	-36	-33	-54	54	-3
1931	-18	72	-50	-30	9
1933	54	6	31	62	-47
1949	-40	-10	33	84	-19
1951	-23	-14	-17	-64	-43
1973	79	-47	-81	-60	-54
1979	30	0	44	30	62
1987	-22	86	56	-82	-65
1993	-66	-54	45	14	26
1997	-72	-27	22	-78	77

TABLE 2. $E_1: y^2 - y = x^3 - x^2$

p	PD
2	(5)
3	(5)
5	(5)
7	(2,5)
13	(2,5)
17	(4,5)
19	(4,5)
23	(25)
29	(2,3,5)
31	(25)
37	(5,7)
41	(2,25)
43	(2,25)
47	(2,4,5)
53	(2,2,3,5)
59	(5,11)
61	(2,25)
67	(3,25)
71	(3,25)
73	(2,5,7)
79	(2,9,5)
83	(2,9,5)
89	(3,25)
97	(3,5,7)
101	(4,5,5)
103	(2,4,3,5)
107	(2,9,5)
109	(4,25)
113	(3,5,7)
127	(8,3,5)
131	(2,3,25)
137	(5,29)
139	(2,5,13)
149	(32,5)
151	(2,3,5,5)
157	(3,5,11)
163	(2,16,5)
167	(4,9,5)
173	(4,9,5)
179	(3,5,13)
181	(25,7)
191	(25,7)
193	(2,5,19)
197	(8,25)
199	(2,4,25)
211	(8,25)
223	(5,41)
227	(2,3,5,7)
229	(5,43)
233	(2,3,5,7)
239	(2,27,5)
241	(2,125)
251	(25,11)
257	(2,2,5,13)
263	(2,125)
269	(2,2,5,13)
271	(4,3,25)
277	(8,5,7)
281	(4,3,25)
283	(8,5,7)
293	(2,27,5)
307	(4,3,25)
311	(2,2,3,25)
313	(9,5,7)
317	(5,61)
331	(25,13)
337	(8,3,3,5)
347	(64,5)
349	(64,5)
353	(3,125)
359	(4,5,19)
367	(5,7,11)
373	(16,25)
379	(5,7,11)
383	(5,7,11)
389	(81,5)
397	(2,8,25)
401	(2,8,25)
409	(8,5,11)
419	(2,8,25)
421	(2,8,25)
431	(2,9,25)
433	(5,89)
439	(16,25)
443	(5,7,13)
449	(5,83)
457	(2,5,47)
461	(2,9,25)
463	(25,19)
467	(9,5,11)
479	(4,5,23)
487	(3,5,31)
491	(4, 125)
499	(2,16,3,5)
* * *	
569	(2,3,5,19)
809	(2,81,5)
1289	(2,3,5,43)
1439	(2,16,9,5)
2539	(2,2,5,127)
3319	(8,5,83)
3559	(8,5,89)
3919	(2,8,5,49)

4.3. *Densities.* For a fixed elliptic curve E defined over the rationals and a fixed prime l, a natural question to ask is, what is the set of primes p such that l divides Card $E(\mathbf{F}_p)$. We will denote this set by $P_l(E)$. We also denote by $\mathrm{Sp}_l(E)$ the set of primes p such that l-primary part splits. If E has complex multiplications, then the splitting field of the l-division equation is abelian over the corresponding imaginary quadratic field; and hence $P_l(E)$ can be characterized by congruences. The elliptic curves investigated here have no complex multiplication, and thus the splitting field of the l-division equation is not solvable in general, and $P_l(E)$ cannot be characterized by congruences; however, the Čebotarev Density Theorem can be applied in this situation to obtain that $P_l(E)$ has density. The actual theoretical computation of the density of $P_l(E)$ is done by using Serre's results concerning the l-division fields associated with E. In the case $l = 2$, we obtain that the Dirichlet Density of $P_2(E_1)$ is 2/3. Furthermore we also get that the density of primes for which the 2-primary component of $E_1(\mathbf{F}_p)$ splits 1/6 (see Heilbronn, p. 228 or Tate-Serre, p. 354 in [6]). A more detailed investigation will appear elsewhere.

The frequences of primes p less than 5000 for which

$$p \in P_l(E) \quad \text{or} \quad p \in \mathrm{Sp}_l(E)$$

for the curves studied here are given in the following table.

TABLE D
(*Relative Frequencies*)

Curve	$2 \mid N_p$	*2-component splits*	$3 \mid N_p$	*3-component splits*	$5 \mid N_p$	$7 \mid N_p$	$E(\mathbf{F}_p)$ *cyclic*	N_p *prime*
E_1	0.67	0.16	0.44	0.018	1.0	0.17	0.62	0
E_2	0.67	0.16	0.44	0.018	1.0	0.17	0.62	0
E_3	0.66	0.16	0.44	0.016	0.24	0.15	0.82	0.063
E_4	0.66	0.15	0.42	0.010	0.22	0.12	0.82	0.07
E_5	1.00	0.49	1.00	0.156	0.23	0.16	0.43	0
E_6	0.67	0.16	0.45	0.017	0.24	0.14	0.83	0.084

The last two columns correspond to the frequencies of primes for which $E(\mathbf{F}_p)$ is cyclic.

4.4. *Theorems and Conjectures.* The above discussion of the numerical results and the tables suggest a few conjectures, some of which we could prove and others which are still open. In Table C we gave some examples of prime pairs (p, q) such that Card $E(\mathbf{F}_p)$ = card $E(\mathbf{F}_p)$. In the computations we found many other occurrences of such pairs which suggest that the number of these pairs is infinite. We also found many triplets.

TABLE 3. $y^2 + xy = x^3 + x^2 - 2x - 7$

p	PD	p	PD	p	PD
2	(2)	167	(4,3,13)	383	(4,7,13)
3	(2)	173	(2,4,3,7)	389	(3,131)
5	(5)	179	(4,3,13)	397	(5,7,11)
7	(2,5)	181	(181)	401	(379)
13	(13)	191	(8,23)	409	(431)
17	(23)	193	(199)	419	(2,11,19)
19	(2,7)	197	(11,19)	421	(409)
23	(2,11)	199	(16,11)	431	(4,3,5,7)
29	(3,7)	211	(8,25)	433	(5,83)
31	(2,17)	223	(4,61)	439	(2,11,19)
37	(41)	227	(4,9,7)	443	(16,29)
41	(47)	229	(13,17)	449	(463)
43	(4,11)	233	(3,5,17)	457	(419)
47	(2,23)	239	(2,9,13)	461	(3,11,13)
53	(9,5)	241	(2,2,5,11)	463	(4,121)
59	(4,13)	251	(2,127)	467	(8,3,19)
61	(2,4,7)	257	(239)	479	(16,31)
67	(2,3,11)	263	(2,11,13)	487	(2,243)
71	(4,3,5)	269	(269)	491	(2,13,19)
73	(2,2,9)	271	(4,9,7)	499	(4,3,41)
79	(2,9,5)	277	(277)	* * *	
83	(2,3,13)	281	(2,2,3,23)		
89	(9,11)	283	(256)	1069	(1069)
97	(3,37)	293	(3,5,19)	1231	(17,7,11)
101	(2,8,7)	307	(2,3,5,11)	1627	(4,11,37)
103	(32,3)	311	(32,9)	1979	(4,9,5,11)
107	(2,3,17)	313	(3,97)	2213	(2213)
109	(121)	317	(2,32,5)	2389	(2389)
113	(3,41)	331	(32,11)	2557	(2557)
127	(16,9)	337	(3,9,13)	3167	(32,9,11)
131	(4,3,11)	347	(64,5)	3613	(3613)
137	(2,2,37)	349	(13,29)	3877	(3877)
139	(2,71)	353	(3,121)		
149	(7,19)	359	(2,181)		
151	(8,3,7)	367	(2,191)		
157	(2,2,3,13)	373	(2,16,11)		
163	(2,83)	379	(4,103)		

TABLE 4. $E_4: y^2 + y = x^3 + x^2$

p	PD	p	PD	p	PD
2	(5)	167	(3,59)	383	(32,11)
3	(2,3)	173	(2,4,3,7)	389	(128,3)
5	(2,5)	179	(32,5)	397	(2,2,101)
7	(8)	181	(2,2,43)	401	(397)
11	(9)	191	(16,13)	409	(2,7,31)
13	(19)	193	(191)	419	(64,7)
17	(3,7)	197	(2,2,49)	421	(16,27)
19	(2,11)	199	(2,3,31)	431	(3,151)
23	(25)	211	(2,3,5,7)	433	(2,223)
29	(4,9)	223	(4,9,7)	439	(9,47)
31	(3,11)	227	(8,29)	443	(2,32,7)
37	(2,19)	229	(5,49)	449	(4,3,5,7)
41	(37)	233	(4,3,19)	457	(4,7,17)
47	(2,2,11)	239	(2,16,7)	461	(2,8,27)
53	(59)	241	(2,127)	463	(4,5,23)
59	(2,4,9)	251	(5,5,11)	467	(2,3,7,11)
61	(4,3,5)	257	(2,3,47)	479	(27,17)
67	(71)	263	(2,3,47)	487	(2,2,113)
71	(2,5,7)	269	(5,59)	491	(2,3,83)
73	(8,3,3)	271	(3,83)	499	(4,127)
79	(2,4,11)	277	(2,5,31)	* * *	
83	(3,23)	281	(263)		
89	(2,47)	283	(263)	541	(541)
97	(7,13)	293	(4,16,5)	1109	(2,3,5,37)
101	(3,37)	307	(9,5,7)	1361	(2,3,227)
103	(103)	311	(27,11)	1429	(1429)
107	(2,4,3,5)	313	(4,73)	1531	(4,383)
109	(103)	317	(3,103)	1657	(1657)
113	(2,67)	331	(2,179)	2069	(2,9,5,23)
127	(127)	337	(11,31)	2087	(2087)
131	(4,31)	347	(64,5)	2281	(2,7,163)
137	(4,3,11)	349	(16,3,7)	2543	(2,8,3,53)
139	(121)	353	(5,7,11)	3011	(2,2,3,251)
149	(2,3,23)	359	(11,31)	3733	(3733)
151	(4,43)	367	(2,8,25)		
157	(8,3,7)	373	(2,9,19)		
163	(2,3,25)	379	(9,41)		

Given an elliptic curve E, it might be of interest to know the density of rational integers n such that $n = \text{card } E(\mathbf{F}_p)$. A related question is that of the density of integers n which can be traces of Frobenius for a given elliptic curve. The last column of Table D shows that except for trivial reasons $E(\mathbf{F}_p)$ is a cyclic group of prime order for a substantial number of primes p. Nevertheless, this frequency seems to tend to zero. For an interesting discussion of a related problem, see Mazur [8].

Another question that arises is that of characterizing which finite abelian groups can be realized as $E(\mathbf{F}_p)$ for some E and some p. Clearly not all finite abelian groups can be so realized, and it would be of interest to know if the obvious necessary condition that each primary part should have rank at most two is also sufficient.

The computations suggest that the number of distinct prime divisors of card $E(\mathbf{F}_p)$ may be large. In this situation we can prove the following:

THEOREM. *We have*

$$\lim_{p} \text{Sup } \omega(N_p) = \infty,$$

where $\omega(n)$ = *number of distinct prime divisors of* n.

The proof of this theorem is given in [2].

TABLE 5. $E_5: y^2 + xy + y = x^3 - x$

p	PD
3	(2,3)
5	(2,3)
11	(2,2,3)
13	(2,9)
17	(4,3)
19	(2,9)
23	(2,4,3)
29	(2,2,9)
31	(4,9)
37	(2,2,9)
41	(4,9)
43	(2,2,9)
47	(4,3,5)
53	(2,8,3)
59	(2,3,11)
61	(2,3,9)
67	(2,4,9)
71	(2,4,9)
73	(8,9)
79	(2,4,9)
83	(2,9,5)
89	(32,3)
97	(4,3,9)
101	(2,3,17)
103	(4,27)
107	(2,16,3)
109	(2,2,27)
113	(2,2,27)
127	(2,8,9)
131	(2,3,19)
137	(2,4,3,5)
139	(2,9,7)
149	(2,4,3,7)
151	(2,8,3,3)
157	(2,3,27)
163	(2,2,3,3,5)

p	PD
167	(4,9,5)
173	(2,3,31)
179	(2,32,3)
181	(2,81)
191	(2,4,3,7)
193	(2,2,9,5)
197	(2,4,27)
199	(4,3,3,5)
211	(2,4,3,9)
223	(8,3,9)
227	(2,3,5,7)
229	(2,9,13)
233	(2,8,3,5)
239	(2,4,27)
241	(4,3,3,7)
251	(2,27,5)
257	(16,3,5)
263	(2,4,3,11)
269	(2,3,47)
271	(32,3,3)
277	(2,16,9)
281	(2,16,9)
283	(2,9,17)
293	(2,27,5)
307	(2,9,17)
311	(16,3,7)
313	(4,81)
317	(2,4,3,13)
331	(2,2,81)
337	(2,2,81)
347	(2,2,3,31)
349	(2,3,9,7)
353	(16,3,7)
359	(2,64,3)
367	(8,9,5)
373	(2,4,9,5)
379	(2,2,9,11)

p	PD
383	(4,3,29)
389	(2,2,3,31)
397	(2,27,7)
401	(2,2,3,5,7)
409	(4,9,11)
419	(2,9,23)
421	(2,8,27)
431	(2,4,3,17)
433	(4,9,13)
439	(16,3,9)
443	(2,4,3,19)
449	(2,8,27)
457	(2,2,9,13)
461	(2,9,25)
463	(2,8,27)
467	(2,3,79)
479	(4,3,43)
487	(2,4,9,7)
491	(2,4,9,7)
499	(2,4,9,7)
* * *	
503	(8,9,7)
1031	(2,4,3,43)
1283	(2,2,3,107)
1487	(16,3,31)
1511	(8,27,7)
1583	(2,8,9,11)
1637	(2,9,7,13)
2039	(2,4,3,5,17)
2087	(2,4,9,29)
2543	(2,8,3,53)
2843	(2,2,9,79)
2903	(8,3,121)
3023	(16,27,7)

The discussion in the preceding paragraphs about the densities leads to the following result. Put:

$\pi(x) = \#$ of primes less than x,

$D_l(x) = \# \{p \leqslant x: p \text{ prime}, l | \text{card } E(\mathbf{F}_p)\}$,

$\widetilde{D}_l(x) = \# \{p \leqslant x: p \in \mathrm{Sp}_l(E)\}$,

$\hat{D}_l(x) = \# \{p \leqslant x: p \equiv -1 \mod l \text{ and } a_p \equiv 0 \mod (l)\}$.

THEOREM. *We have for almost all primes* l

$$\lim_{x\to\infty} D_l(X)/\pi(x) = C_l, \qquad \lim_{x\to\infty} \widetilde{D}_l(x)/\pi(x) = \widetilde{C}_l, \qquad \lim_{x\to\infty} \hat{D}_l(x)/\pi(x) = \hat{C}_l,$$

where

$$C_l > \widetilde{C}_l = 2/(l-1)^2 l(l+1) \quad \textit{and} \quad \hat{C}_l > 0.$$

The proof of this theorem will appear elsewhere.

For an elliptic curve E, $E(\mathbf{F}_p)$ is cyclic if each of its primary parts is of rank one. Therefore, we conjecture that the set of primes for which $E(\mathbf{F}_p)$ is cyclic has a density given by $C(E) = \Pi_l^*(1 - \widetilde{C}_l)$, where * means that some correction should be made for the exceptional primes in the preceding theorem which is also the same as the set of exceptional primes in Serre's Theorem. Clearly $C(E)$ could be zero for trivial reasons

TABLE 6. E_6: $y^2 + y = x^3 - x$

p	PD	p	PD	p	PD
2	(5)	167	(4,9,5)	383	(4,7,13)
3	(7)	173	(3,5,11)	389	(2,193)
5	(8)	179	(2,81)	397	(13,31)
7	(9)	181	(3,59)	401	(128,3)
11	(17)	191	(4,49)	409	(2,3,5,13)
13	(16)	193	(4,5,11)	419	(7,59)
17	(2,9)	197	(3,5,13)	421	(2,223)
19	(4,5)	199	(2,9,11)	431	(2,3,7,11)
23	(2,11)	211	(9,25)	433	(25,17)
29	(8,3)	223	(241)	439	(4,103)
31	(4,9)	227	(4,61)	443	(443)
41	(3,17)	229	(223)	449	(2,9,23)
43	(2,3,7)	233	(2,2,3,19)	457	(8,5,11)
47	(3,19)	239	(2,3,41)	461	(16,27)
53	(53)	241	(4,3,19)	463	(2,243)
59	(4,13)	251	(2,127)	467	(2,5,47)
61	(2,5,7)	257	(2,3,43)	479	(2,233)
67	(2,2,3,5)	263	(5,49)	487	(512)
71	(9,7)	269	(2,2,3,23)	491	(2,4,5,13)
73	(3,25)	271	(3,101)	499	(8,61)
79	(4,19)	277	(2,7,19)		* * *
83	(9,11)	281	(2,27,5)		
89	(2,43)	283	(8,5,7)	577	(2,289)
97	(2,47)	293	(2,4,37)	599	(599)
101	(9,11)	307	(25,13)	2243	(4,3,11,17)
103	(2,43)	311	(8,3,13)	3511	(2,4,439)
107	(2,4,3,5)	313	(4,73)	3989	(3989)
109	(2,9,7)	317	(2,4,37)	3541	(3643)
113	(4,3,11)	331	(2,167)		
127	(127)	337	(3,121)		
131	(16,9)	347	(2,179)		
137	(2,8,9)	349	(2,4,43)		
139	(2,4,17)	353	(2,173)		
149	(5,31)	359	(3,125)		
151	(2,4,17)	367	(2,4,9,5)		
157	(27,5)	373	(3,131)		
163	(2,7,13)	379	(5,73)		

as happens, for example, for some of the modular curves, but the conjecture still makes sense once we divide E by a suitable subgroup; for example, we can ask for the density of primes p such that the group $(E_1/H)(\mathrm{F}_p)$ is cyclic, where H is the subgroup of order 5 generated by (0, 0).

Department of Mathematics
Texas A & M University
College Station, Texas 77843

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

1. B. J. BIRCH, *Elliptic Curves and Modular Functions,* Symposia Mathematica, vol. IV, (INDAM, Rome, 1968/69), Academic Press, London, 1970. MR 42 #4549.

2. I. BOROSH, C. MORENO & H. PORTA, "Elliptic curves over finite fields. I," *Proceedings of the* 1972 *Number Theory Conference,* Boulder, Colorado.

3. I. BOROSH, C. MORENO & H. PORTA, "Elliptic curves over finite fields. III." (In preparation.)

4. J. BRILLHART & I. GERST, "On the prime divisors of polynomials," *Amer. Math. Monthly,* v. 78, 1971, pp. 250–266. MR 43 #4797.

5. J. W. S. CASSELS, "Diophantine equations with special reference to elliptic curves," *J. London Math. Soc.,* v. 41, 1966, pp. 193–291; Corrigenda, *ibid.,* v. 42, 1967, p. 183. MR 33 #7299; 34 #2523.

6. J. W. S. CASSELS & A. FRÖHLICH (Editors), *Algebraic Number Theory*, Academic Press, London; Thompson Book, Washington, D. C., 1967. MR 35 #6500.

7. K. DOI & H. NAGANUMA, "On the algebraic curves uniformized by arithmetical automorphic functions," *Ann. of Math.* (2), v. 86, 1967, pp. 449–460. MR 36 #2618.

8. B. MAZUR, "Rational points of abelian varieties," *Invent. Math.*, v. 18, 1972, pp. 183–266.

9. A. P. OGG, "Rational points on certain elliptic modular curves," *Number Theory Symposium*, St. Louis, 1972.

10. J.-P. SERRE, "Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques," *Invent. Math.*, v. 15, 1972, pp. 259–331.

11. G. SHIMURA, "A reciprocity law in non-solvable extensions," *J. Reine Angew. Math.*, v. 221, 1966, pp. 209–220. MR 32 #5637.

12. J. VÉLU, "Courbes elliptiques sur Q ayant bonne réduction en dehors de $\{11\}$," *C. R. Acad. Sci. Paris Sér. A-B*, v. 273, 1971, pp. A73–A75. MR 47 #5004.

13. B. F. WYMAN, "What is a reciprocity law?," *Amer. Math. Monthly*, v. 79, 1972, pp. 571–586. MR 46 #7199.