On a Conjecture of Zarhin Concerning the Existence of Isogenic but Non-Isomorphic Elliptic Curves over Finite Fields and a General Algorithm for Computing Elliptic Curves over Finite Fields with Respect for Isomorphism.

TIMOTHY NATHANIEL TRUDELL and JONATHAN DOUGLAS BARRY[1]

Definition. *An **elliptic curve** E over a field $\mathbb{F}$ is a nonsingular cubic curve*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

having coefficients in $\mathbb{F}$ together with a point $O \in E$ and the algebraic group law on E defined by O and the chord-tangent law of composition for two points P, $Q \in E$ given by the relation $P + Q = O(PQ)$. Here PQ denotes the third point of intersection between E and the line in the projective plane through the points P and Q; $O(PQ)$ denotes the third point of intersection between PQ and the point at infinity O [Husemöller 15].

For an elliptic curve E over a finite field $\mathbb{F}_p$ of prime characteristic $p \geq 5$, E can be written in the particularly simple form (due to Weierstraß)

$$y^2 = x^3 + a_4x + a_6 \tag{2}$$

where $a_4, a_6 \in \mathbb{F}_p$.

Algebraic geometry is the primary tool employed to develop the properties of elliptic curves; we shall make a brief synopsis of the general theory as it applies to our research.

Associated to any elliptic curve E is a modular form due to Jacobi called the *j-invariant*. For an elliptic curve over a finite field $\mathbb{F}_p$ with $p \geq 5$, the j-invariant is given by the formula

$$j(E) = 12^3 \frac{4a_4^3}{4a_4^3 + 27a_6^2}. \tag{3}$$

It is invariant with respect to the isomorphism class of the curve E; i.e., two curves isomorphic over a given field will always have the same j-invariant.

The other key quantity associated to an elliptic curve is its algebraic *discriminant* Δ. For an elliptic curve over a finite field $\mathbb{F}_p$ with $p \geq 5$, the discriminant is given by the formula

$$\Delta = -16(4a_4^3 + 27a_6^2). \tag{4}$$

In general, an elliptic curve E will be smooth if and only if its discriminant does not vanish. Curves having vanishing discriminants are thus singular, and we shall have little more to say here about such singular curves.

[1]The Pennsylvania State University, University Park, PA 16802. USA

¿From these basic definitions, we can formulate a crude algorithm for computing elliptic curves over fields of small characteristic p. For the present time, we shall assume that all of our finite fields have *order* p in addition to characteristic p; this will prevent any complications arising from field extensions. Our method will be to consider the p^2 curves of the form $y^2 = x^3 + a_4x + a_6$, ascertaining first by the discriminant criterion which of these are singular, and then to determine the j-invariant for the other nonsingular curves.

Definition. *An* ***admissible change of variables*** A *for an elliptic curve* E *is a transformation of the form*

$$A: \quad x = u^2\bar{x} + r, \quad y = u^3\bar{y} + su^2\bar{x} + t, \tag{5}$$

where $u, r, s, t \in \mathbb{F}_p$ and $u \neq 0$.

By elementary algebraic considerations, an admissible change of variables acting on an elliptic curve E will map E to another elliptic curve $\bar{E}$ having the same j-invariant [Husemöller 68].

Definition. *Two elliptic curves* E *and* $\bar{E}$ *are* ***isomorphic*** $(E \cong \bar{E})$ *over a field* $\mathbb{F}_p$ *if there exists an admissible change of variables* A *such that* $A(E) = \bar{E}$.

Because isomorphism is an equivalence relation, it is evident that if there exists an A such that $A(E) = \bar{E}$ then there also exists an A' with $A'(\bar{E}) = E$. In particular, then, A is an invertible transformation, and this is the reason for demanding $u \neq 0$ in the definition of an admissible change of variables. The general condition on isomorphism can be made more specific for elliptic curves over finite fields $\mathbb{F}_p$ with $p \geq 5$, as in the following theorem.

Theorem. *For elliptic curves* $E: \ y^2 = x^3 + a_4x + a_6$ *and* $\bar{E}: \ y^2 = x^3 + \bar{a_4}x + \bar{a_6}$ *having the same* j*-invariant over a field* $\mathbb{F}_p$ *of characteristic* $p \geq 5$, $E \cong \bar{E}$ *if and only if there exists some* $u \in \mathbb{F}_p$ *with:*

$$\frac{a_4\bar{a_6}}{\bar{a_4}a_6} = u^2 \ \ (j \neq 0, 12^3); \ \ \frac{a_4}{\bar{a_4}} = u^4 \ \ (j = 12^3); \ \ \frac{a_6}{\bar{a_6}} = u^6 \ \ (j = 0). \tag{6}$$

Proof. We have E given by $y^2 = x^3 + a_4x + a_6$ and $\bar{E}$ by $y^2 = x^3 + \bar{a_4}x + \bar{a_6}$. In considering this Weierstraß form of the elliptic curve, we have implicitly assumed that the field $\mathbb{F}_p$ has characteristic $p \geq 5$ (this is also explicitly stated in the hypothesis). Hence, we have that the coefficients a_1, a_2, and a_3 vanish; then for φ an isomorphism with $\varphi : E \to \bar{E}$, by the rule for an admissible change of variables we must have

$$\varphi(x) = u^2\bar{x} \qquad \varphi(y) = u^3\bar{y} \qquad a_4 = u^4\bar{a_4} \qquad a_6 = u^6\bar{a_6}. \tag{7}$$

Now if $j \neq 0$ and $j \neq 12^3$, by (3) we have immediately that $a_4 \neq 0$, since this would imply $j = 0$, and also, $a_6 \neq 0$ since this would imply that $j = 12^3$. In this

case, (7) implies, since u is invertible, that we must have $\frac{a_4}{\bar{a}_4} = u^4$ and $\frac{\bar{a_6}}{a_6} = u^{-6}$; an equivalent way of formulating this is to say $(\frac{a_4}{\bar{a}_4})(\frac{\bar{a_6}}{a_6}) = u^4u^{-6} = u^{-2}$, or $\frac{a_4\bar{a_6}}{\bar{a}_4 a_6} = u^2$ for some $u \in \mathbb{F}_p$. For $j = 12^3$, we see immediately that the fractional part of (3) must tend to unity, which in turn implies that $a_6 = 0$. From this observation, (7) gives that we must have $\frac{a_6}{\bar{a_6}} = u^6$ for some $u \in \mathbb{F}_p$. Finally for $j = 0$, we have by (3) that $a_4 = 0$ and hence $E \cong \bar{E}$ if and only if $\frac{a_4}{\bar{a}_4} = u^4$ for some $u \in \mathbb{F}_p$, **Q.E.D.**

Now that we have established the notion of isomorphism on elliptic curves, we note without proof the following theorem.

Theorem. *For elliptic curves E and $\bar{E}$, if $E \cong \bar{E}$ then there exists an isomorphism $f : P \mapsto \bar{P}$ mapping the group of points $P = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : (x, y) \in E\}$ on E to the set of points $\bar{P} = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : (x, y) \in \bar{E}\}$ on $\bar{E}$.*

Indeed, this theorem justifies our somewhat periphrastic use of the term *isomorphic* to describe classes of elliptic curves that are invariant under an admissible change of variables, for these are precisely the curves that preserve the chord-tangent group law among the points on the respective curves.

We can now extend our algorithm from above to consider classes of isomorphic curves over a given field $\mathbb{F}_p$. We merely have to use (3) to compute the j-invariant, and then to consider the appropriate case of (6) to determine whether the two curves in question are isomorphic. For a given finite algebraic field of low characteristic p, a simple computer program like the one we have written below can quickly calculate all elliptic curves over the field respective of isomorphism in a relatively short amount of time.

We have one final preliminary definition, which is integral to what follows.

Definition. *Two elliptic curves E and $\bar{E}$ are **isogenic** (or **isogenous**) if there exists a rational map*

$$\xi = \frac{\sum_{\forall m=i+j} a_m x^i y^j}{\sum_{\forall n=i+j} b_n x^i y^j}, \quad \forall a_m, b_n \in \mathbb{F}_p \tag{8}$$

such that $\xi : E \mapsto \bar{E}$ with $\xi(O) = \bar{O}$, where O and $\bar{O}$ denote the points at infinity (the zero points for the group law) on E and $\bar{E}$, respectively.

We are now in a position to formulate the fundamental question at hand for our research. It is evident from the above discussion that two elliptic curves E and $\bar{E}$ that are isomorphic to one another over some finite field are evidently isogenic to one another, since in particular there is a rational map ξ given simply by the admissible change of variables (5). The converse of this statement is another matter. Zarhin has conjectured that there do indeed exist elliptic curves that are isogenic to one another but not isomorphic over a given finite field. We aim to find such a class of elliptic curves using a computer algorithm focusing on the rational points of such curves.

An important step in finding the curves that we seek is the following theorem, whose proof is omitted.

Theorem. *Two elliptic curves E and $\bar{E}$ are isogenic over a finite field $\mathbb{F}_p$ if and only if they have equally many points defined over $\mathbb{F}_p$* [Wittmann 339].

The reference to points in the above theorem includes both rational points as well as points in any field extension. Since presently we are restricting ourselves to the consideration of prime fields, the set of rational points is in fact the set of all points from $\mathbb{F}_p$ on the curve E, and in this special case of prime fields, the above theorem reduces to the condition that both curves have equally many rational points in the field $\mathbb{F}_p$.

Now our computer algorithm takes over to find the curves that we seek. We illustrate the computational processes with the case of $\mathbb{F}_5$, the field having both characteristic and order $p = 5$. The computer first employs (3) to output a $p \times p$ matrix having the j-invariants of all possible elliptic curves. In this array, each entry (a_4, a_6) (beginning with $(0, 0)$ in the upper left corner and ending with $(p - 1, p - 1)$ in the lower right corner) denotes an elliptic curve of the form $E:\ y^2 = x^3 + a_4x + a_6$; curves that are singular by (4) are arbitrarily assigned the value $p + 1$ in the matrix and do not play any further role in the algorithm. The matrix looks like this:

$$\begin{array}{ccccc} 6 & 0 & 0 & 0 & 0 \\ 3 & 2 & 1 & 1 & 2 \\ 3 & 4 & 6 & 6 & 4 \\ 3 & 6 & 4 & 4 & 6 \\ 3 & 1 & 2 & 2 & 1 \end{array} . \tag{9}$$

¿From the discussion following (3) above, we know immediately that curves having different j-invariants cannot be isomorphic; hence we have only to resolve the question of which curves having the same j-invariant are isomorphic over the given field. To this end, we employ an algorithm that takes curves having the same j-invariant and determines from (6) whether or not they are pairwise isomorphic to one another. In this case, we obtain the following results:

$$\begin{array}{ll} j = 0: & (0,1) \cong (0,4) \quad (0,2) \cong (0,3) \\ j = 1: & (1,2) \cong (1,3) \quad (4,1) \cong (4,4) \\ j = 2: & (1,1) \cong (1,4) \quad (4,2) \cong (4,3) \\ j = 3: & \text{(none are isomorphic)} \\ j = 4: & (2,1) \cong (2,4) \quad (3,2) \cong (3,3) \end{array} . \tag{10}$$

Having classified all curves over the field $\mathbb{F}_5$ respective of isomorphism, we have only to determine in which isogeny class each curve lies. To this end, a third algorithm we have written computes the rational points from $\mathbb{F}_5 \times \mathbb{F}_5$ that are on each elliptic curve E. From the second theorem above, we should only consider curves having the same number of rational points, as this condition is equivalent to isogeny for prime fields. In the case of $\mathbb{F}_5$, the isogenic curves are the following (we are omitting the pairs which are known to be isomorphic from

(10), since isomorphic curves are evidently isogenic):

$$\begin{array}{ll} \{(1,0),(1,2)\} & (4 \text{ points}) \\ \{(0,1),(0,2)\} & (6 \text{ points}) \\ \{(4,0),(4,1)\} & (8 \text{ points}) \end{array} . \tag{11}$$

For the first and third pairs of elliptic curves given in (11), the question of whether the curves' sets of points have the same group structure cannot be determined by inspection, since respective of isomorphism there are two (abelian) groups of order four (namely, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$) and there are three (abelian) groups of order eight (namely, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$). Hence, it is entirely possible that the groups of points on these pairs of elliptic curves are not isomorphic. This same argument does not apply, however, to the second pair of curves in (11). For there is only one algebraic group of order six, namely $\mathbb{Z}_6$. Hence we have found the first example of the kind of curves that we seek:

$$y^2 = x^3 + 1 \quad \text{and} \quad y^2 = x^3 + 2 \tag{12}$$

are isogenic, non-isomorphic curves over $\mathbb{F}_5$ whose sets of points have isomorphic group structures. (It turns out the pair of curves $y^2 = x^3 + 4x$ and $y^2 = x^3 + 4x + 1$ do not have isomorphic groups of points; the former group is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ while the latter is $\mathbb{Z}_8$.)

An analogous set of calculations on the field of seven elements $\mathbb{F}_7$ gives us another pair of curves having the desired properties, namely

$$y^2 = x^3 + 5 \quad \text{and} \quad y^2 = x^3 + 3x + 5. \tag{13}$$

These curves are not isomorphic over the field of seven elements, since (3) gives immediately that they have different j-invariants, the first having $j = 0$ and the latter having $j = 3$. Yet they do indeed have the same group structure, namely that of $\mathbb{Z}_7$.

It turns out that the kind of curves that we seek are quite prevalent in the prime fields. Our computer algorithm processed elliptic curves in $\mathbb{F}_p$, $p \leq 409$ (this is the eightieth prime number) and discovered at least one such pair in all of these fields (these pairs of elliptic curves are listed in the appendix of this paper). In most cases there are several such pairs. Hence, we conjecture that there always exists such a pair of isogenic, non-isomorphic curves for sufficiently small p. We must be careful to stress that this conjecture is made only for fields $\mathbb{F}_p$ where $O(p) \approx 100$, since in general, by the first theorem above, over larger and larger finite fields, there is a greater probability that two elliptic curves will be isomorphic as curves. More precisely, in the limit of extension (or closure) for $\mathbb{F}_p$, we shall have that all curves are isomorphic, since $\overline{\mathbb{F}}_p$ contains all roots of all irreducible polynomials of all degrees from $\mathbb{F}_p$.

We can also consider quadratic field extensions of $\mathbb{F}_p$ by admitting a root of a quadratic polynomial irreducible over $\mathbb{F}_p$ and then completing the field to obtain an extension field $\mathbb{F}_{p^2}$, which still has characteristic p. For the quadratic extensions with $p = 3$ and $p = 5$, our computer algorithm discovered that there

do not exist isogenic but non-isomorphic pairs of elliptic curves in these fields. This curious phenomenon may be a local behavior, i.e., there may actually exist such pairs of curves in quadratic extension fields for larger prime numbers p, but we were unable to further investigate the question.

To conclude, we would like to suggest that this work would not have been possible without the kind and generous assistance of numerous people. We would first like to thank the National Science Foundation for supporting our effort through the *Vertical Integration of Reseach and Education in the Mathematical Sciences* (VIGRE) grant. We would also like to thank Dr. Misha Guysinsky of Penn State University for the helpful comments he offered us on a daily basis concerning the direction our work should take, and Dr. Yuri G. Zarhin, also of Penn State University, who first suggested this particular problem to us and so graciously and patiently answered all of our questions about elliptic curves. Finally, we would like to thank Flossie Dunlop, REU/MASS secretary, for her generous and able assistance in the preparation of our talk on this subject at the MASS-Fest 2003, held at Penn State University, University Park, Pennsylvania on August 5-6, 2003.

References.

1. D. Husemöller, "Elliptic Curves," Springer-Verlag, New York, 1987.

2. C. Wittmann,"Group Structure of Elliptic Curves over Finite Fields" *Journal of Number Theory* **88**, 335-344 (2001).

University Park, PA
August 7, 2003.