

# CLASS NUMBERS OF $p$ -GROUPS OF A GIVEN ORDER

Nigel Boston and I. M. Isaacs

## 1. Introduction.

If  $G$  is a finite group, then as usual, we write  $k(G)$  to denote the number of conjugacy classes of  $G$ . Given a positive integer  $m$ , there are, of course, only finitely many isomorphism types of groups of order  $m$ , and so we can write  $D(m)$  to denote the number of different numbers  $k(G)$  that arise as  $G$  runs over all groups of order  $m$ . In this paper, our concern is with  $p$ -groups, where  $p$  is prime, and we study the behavior of  $D(p^e)$  as  $p$  varies while the exponent  $e$  is held constant.

We begin with some small exponents. Since for each prime  $p$ , there is just one isomorphism type of groups of order  $p$ , it is clear that  $D(p) = 1$ . Also, although there are two isomorphism types of groups of order  $p^2$ , each group of this order is abelian, and so  $k(G) = p^2$  for all such groups, and hence  $D(p^2) = 1$ . Next, consider groups of order  $p^3$ . There are five isomorphism types of groups of this order: three are abelian and two are not. Of course,  $k(G) = p^3$  for the three abelian groups, and for the two nonabelian groups of order  $p^3$ , it is not hard to see that  $k(G) = p^2 + p - 1$ . We conclude, therefore, that  $D(p^3) = 2$  for all primes  $p$ . There are 15 isomorphism types of order  $p^4$  (except when  $p = 2$ , when there are just 14) but for each such group,  $k(G)$  is one of the three numbers  $p^4$ ,  $p^3 + p^2 - p$  or  $2p^2 - 1$ . Since each of these possibilities actually occurs for some group of order  $p^4$ , it follows that  $D(p^4) = 3$  for all primes  $p$ .

The situation is more interesting for groups of order  $p^5$ . If  $p = 2$ , there are 51 isomorphism types; if  $p = 3$ , there are 67 isomorphism types and for  $p \geq 5$ , the number of isomorphism types is  $61 + 2p + 2 \gcd(p - 1, 3) + \gcd(p - 1, 4)$ . In particular, the number of isomorphism types is unbounded for large  $p$ , but nevertheless, for each prime, there are at most six possible numbers of conjugacy classes among these groups. In fact, if  $|G| = p^5$ , it is known that  $k(G)$  must be one of the numbers  $p^5$ ,  $p^4 + p^3 - p^2$ ,  $p^4 + p - 1$ ,  $2p^3 - p$ ,  $p^3 + p^2 - 1$  or  $2p^2 + p - 2$ . Except when  $p = 2$ , all of these possibilities actually occur for each prime  $p$ , and since for each prime, these six formulas yield six different numbers, it follows that  $D(p^5) = 6$  for  $p > 2$ . But  $D(2^5) = 5$  since there is no group of order  $2^5$  that has exactly  $2p^2 + p - 2 = 8$  classes.

Similarly, one can establish that  $D(p^6) = 11$  for  $p > 3$ , while  $D(3^6) = 10$  and  $D(2^6) = 9$ . What happens in this case is that there are eleven different polynomials in  $p$  that can occur as  $k(G)$  when  $|G| = p^6$ . Two of these happen to equal 19 when  $p = 2$ , and one of the polynomials does not occur as a class number when  $p = 2$  or  $p = 3$ .

These examples suggest that perhaps for each exponent  $e$ , the number  $D(p^e)$  is eventually constant, or at least that it is bounded as  $p$  gets large. The main result of this paper shows that this is incorrect.

**THEOREM A.** *The number  $D(p^9)$  approaches infinity as  $p$  approaches infinity.*

For each prime  $p$ , we construct a particular family of groups of order  $p^9$ , and we will see that as the prime  $p$  approaches infinity, the number of different numbers of conjugacy classes among the groups in each family approaches infinity. We mention that each of our groups has nilpotence class 2, and for  $p > 2$ , each of them has exponent  $p$ . In particular, it

follows that the number of isomorphism types of class 2, exponent  $p$  groups of order  $p^9$  is unbounded as  $p$  gets large. Also, although we will not pursue this here, even the number of isoclinism classes of these groups is unbounded. (We mention that isoclinism is an equivalence relation among groups that is weaker than isomorphism, but that nevertheless, isoclinic groups of equal orders have equal numbers of classes.)

According to private communications from Eamonn O'Brien, to whom we are grateful, it is known that  $D(p^7)$  is bounded, and he believes that  $D(p^8)$  is probably bounded too. It appears, therefore, that  $e = 9$  is the smallest exponent for which  $D(p^e)$  is unbounded as a function of the prime  $p$ .

We close this introduction by mentioning that the problem of determining the behavior of  $D(p^e)$  as  $p$  varies was called to our attention by Edith Adan-Bante. We thank her for alerting us to this interesting problem.

## 2. Some groups.

Let  $F$  be a field of order  $p$ , where  $p$  is prime, and fix positive integers  $m$  and  $n$ . For each subspace  $S$  of the space of  $m \times n$  matrices over  $F$ , we construct a group  $G = G(S)$  as follows. First, for each matrix  $X \in S$ , define the  $(m+n) \times (m+n)$  matrix  $a(X)$  by

$$a(X) = \begin{bmatrix} I_m & X \\ 0 & I_n \end{bmatrix},$$

where  $I_m$  and  $I_n$  are respectively the  $m \times m$  identity matrix and the  $n \times n$  identity matrix. Then the set  $A = A(S) = \{a(X) \mid X \in S\}$  is an elementary abelian subgroup of order  $p^k$  in  $GL(m+n, F)$ , where  $k = \dim_F(S)$ . Let  $B$  be the  $(m+n)$ -dimensional row space over  $F$  and observe that  $A$  acts by right multiplication on  $B$ , and so we can construct the semidirect product  $G = B \rtimes A$ , which is a group of order  $p^{m+n+k}$ .

In order to compute the class number  $k(G(S))$ , we observe that in general, for an arbitrary finite group  $G$ , we have

$$k(G) = \frac{1}{|G|} \sum_{x \in G} |\mathbf{C}_G(x)|.$$

In our situation, the following lemma is relevant.

**(2.1) LEMMA.** *Let  $G = AB$ , where  $A \subseteq G$  and  $B \triangleleft G$  are abelian subgroups such that  $A \cap B = 1$ . If  $a \in A$  and  $b \in B$ , then  $|\mathbf{C}_G(ab)|$  is equal to the number of ordered pairs  $(x, y)$ , where  $x \in A$ ,  $y \in B$  and  $[y, a] = [b, x]$ .*

**Proof.** Every element of  $G$  is uniquely of the form  $xy$ , where  $x \in A$  and  $y \in B$ , and so to compute  $|\mathbf{C}_G(ab)|$ , we need to compute the number of pairs  $(x, y)$  with  $x \in A$  and  $y \in B$  such that  $ab$  commutes with  $xy$ .

Now  $(ab)(xy) = axb^xy$  and  $(xy)(ab) = xay^ab$ . Since  $ax = xa$ , we see that a necessary and sufficient condition that  $(ab)(xy) = (xy)(ab)$  is that  $b^xy = y^ab$ . Since  $B$  is commutative and  $b^x, b, y^a$  and  $y$  all lie in  $B$ , it follows that  $ab$  and  $xy$  commute precisely when  $b^{-1}b^x = y^{-1}y^a$ , and this completes the proof. ■

To apply Lemma 2.1 in our situation, where  $G = G(S)$ , we need to compute commutators of the form  $[b, a]$ , where  $b \in B = F^{m+n}$  and  $a = a(X) \in A$  is a certain  $(n+m) \times (n+m)$  matrix. To do this, we view the row space  $B$  as the direct sum of the  $m$ -dimensional row space  $F^m$  and the  $n$ -dimensional row space  $F^n$ , and we write  $b = (v, w)$ , where  $v \in F^m$  corresponds to the first  $m$  components of  $b$  and  $w \in F^n$  corresponds to the last  $n$  components. The conjugate  $b^a$  in  $G$  is the row vector  $b \cdot a = (v, v \cdot X + w)$ , and thus the commutator  $[b, a] = -b + b \cdot a = (0, v \cdot X)$ .

Applying Lemma 2.1, we see now that if  $b = (v, w)$  and  $a = a(X)$ , then  $|\mathbf{C}_G(ab)|$  is  $p^n$  times the number of pairs  $(u, Y)$ , where  $u \in F^m$  and  $Y \in S$  and  $v \cdot Y = u \cdot X$ . (The factor  $p^n$ , of course, is due to the fact that each row vector  $u \in F^m$  is the  $F^m$  component of exactly  $p^n$  different elements of  $B = F^{m+n}$ .) For notational convenience, we write  $f(v, X)$  to denote the number of pairs  $(u, Y)$  such that  $u \cdot X = v \cdot Y$ , where  $u, v \in F^m$  and  $X, Y \in S$ .

We see now that if  $G = G(S)$ , then

$$k(G) = \frac{1}{|G|} \sum_{a,b} |\mathbf{C}_G(ab)| = \frac{p^{2n}}{p^{m+n+k}} \sum_{v,X} f(v, X),$$

where the first sum runs over  $a \in A$  and  $b \in B$  and the second runs over  $v \in F^m$  and  $X \in S$ . The extra factor of  $p^n$  counts the number of elements  $b \in B$  whose first  $m$  coordinates form the vector  $v$ .

Our next task is to compute  $f(v, X)$ , where  $v \in F^m$  and  $X \in S$ . For this purpose, we define the **range** of  $X$  to be the subspace of  $F^n$  given by  $R(X) = \{v \cdot X \mid v \in F^m\}$ . Also, for a fixed space  $S$  of  $m \times n$  matrices, we define the **range** of a vector  $v \in F^m$  to be  $R(v) = \{v \cdot X \mid X \in S\}$ , which is also a subspace of  $F^n$ .

**(2.2) LEMMA.** *Let  $v \in F^m$  and  $X \in X$  and write  $e = e(v, X) = \dim_F(R(v) + R(X))$ . Then  $f(v, X) = p^{m+k-e}$ , where  $k = \dim(S)$ .*

**Proof.** We need to count pairs  $(u, Y)$  such that  $u \cdot X = v \cdot Y$ . If  $(u, Y)$  is such a pair, then clearly, the row vector  $u \cdot X = v \cdot Y$  lies in both  $R(v)$  and  $R(X)$ , and so we write  $D = R(v) \cap R(X)$  and we let  $d = \dim(D)$ . For each vector  $w \in D$ , the set of vectors  $u \in F^m$  such that  $u \cdot X = w$  is a coset of the kernel of the linear transformation  $u \mapsto u \cdot X$  from  $F^m$  to  $F^n$ , and the dimension of this kernel is  $m - \dim(R(X))$ . Given  $w \in D$ , therefore, the number of possibilities for  $u$  is  $p^{m - \dim(R(X))}$ . Similarly, the set of matrices  $Y \in S$  such that  $v \cdot Y = w$  is a coset of the kernel of the linear transformation  $Y \mapsto v \cdot Y$  from  $S$  to  $F^n$ , and this kernel has dimension  $k - \dim(R(v))$ . Given  $w \in D$ , therefore, the number of possibilities for  $Y$  is  $p^{k - \dim(R(v))}$ . The number of ordered pairs  $(u, Y)$  such that  $u \cdot X = w = v \cdot Y$  is therefore equal to  $p^{m+k - \dim(R(v)) - \dim(R(X))}$ , and we see that to compute  $f(v, X)$ , we must multiply this quantity by  $p^d$ , which is the number of choices for  $w \in D$ . Since  $\dim(R(v)) + \dim(R(X)) = d + e$ , the result follows. ■

Combining our results so far, we have the following.

**(2.3) COROLLARY.** *Using the notation that we have established, we have*

$$k(G(S)) = \sum_{v,X} p^{n - e(v,X)},$$

where the sum runs over  $v \in F^m$  and  $X \in S$ .

Note that  $e(v, X)$  is the dimension of the subspace  $R(v) + R(X)$  of  $F^n$ , and thus each of the exponents  $n - e(v, X)$  is nonnegative.

### 3. Spaces of matrices.

Now set  $m = n = k = 3$ . Our task is to construct a number of 3-dimensional spaces  $S$  of  $3 \times 3$  matrices over the field  $F$  of order  $p$  such that for large primes  $p$  we obtain a large number of different values for the class number  $k(G(S))$  as  $S$  varies. All of the groups  $G(S)$ , of course, will have order  $p^{m+n+k} = p^9$ .

Given a nonzero element  $a \in F$ , let  $S_a$  be the space of matrices of the form

$$X = X(x, y, z) = \begin{bmatrix} x & y & az \\ z & x & y \\ z & 0 & x \end{bmatrix},$$

for  $x, y, z \in F$ .

In order to use Corollary 2.3, we will have to compute the dimensions of subspaces of  $F^3$  of the form  $R(v) + R(X)$ , where  $X \in S_a$  and  $v \in F^3$  is an arbitrary row vector. Of course,  $R(X)$  is exactly the row space of the matrix  $X$ , and it is also convenient to view  $R(v)$  as the row space of a certain matrix, as follows. If  $r, s, t \in F$ , we observe that

$$[r \ s \ t] \begin{bmatrix} x & y & az \\ z & x & y \\ z & 0 & x \end{bmatrix} = [x \ y \ z] \begin{bmatrix} r & s & t \\ 0 & r & s \\ s+t & 0 & ar \end{bmatrix}.$$

If we define

$$Y = Y(r, s, t) = \begin{bmatrix} r & s & t \\ 0 & r & s \\ s+t & 0 & ar \end{bmatrix},$$

therefore, we see that  $R(v)$  is exactly the row space  $R(Y)$  of the matrix  $Y = Y(r, s, t)$ , where  $v = [r \ s \ t]$ . We let  $T_a$  be the space of matrices of this form, so that  $T_a$ , like  $S_a$ , is a 3-dimensional space of matrices. To apply Corollary 2.3, therefore, we need to consider the spaces of the form  $R(X) + R(Y)$ , where  $X \in S_a$  and  $Y \in T_a$ .

Of course, the row space of a nonzero matrix  $X$  remains unchanged if the matrix is replaced by a nonzero scalar multiple. We refer to the set of such multiples as the **line** of matrices determined by  $X$ . Each line, therefore, contains exactly  $p - 1$  matrices, and the sets of nonzero matrices in each of the spaces  $S_a$  and  $T_a$  are partitioned into  $p^2 + p + 1$  lines.

The key result that we will use to compute  $k(G(S_a))$  is the following.

**(3.1) THEOREM.** *Let  $0 \neq a \in F$ . Then each nonzero matrix in  $S_a$  and each nonzero matrix in  $T_a$  has rank 2 or rank 3. Also, for matrices  $X \in S_a$  and  $Y \in T_a$ , the relation  $R(X) = R(Y)$  defines a one-to-one correspondence between the set of lines of rank 2 matrices in  $S_a$  and the set of lines of rank 2 matrices in  $T_a$ . In particular, the spaces  $S_a$  and  $T_a$  contain equal numbers of lines of rank 2 matrices.*

**Proof.** First, we consider the nonzero matrices  $X = X(x, y, z)$  for which  $z = 0$ . If  $x \neq 0$ , it is clear that  $X$  has rank 3. On the other hand, if  $x = 0$ , then since  $X$  is nonzero we must have  $y \neq 0$ , and thus  $X$  has rank 2. This accounts for one line of matrices of rank 2 in  $S_a$ , and it is clear that for matrices  $X$  in this line, the row space  $R(X)$  is exactly the set of vectors with first entry 0.

Now consider the nonzero matrices  $Y = Y(r, s, t)$  for which  $s + t = 0$ . Since  $a \neq 0$ , we see that  $Y$  has rank 3 if  $r \neq 0$ . If  $r = 0$ , then necessarily  $s \neq 0$  since otherwise  $t = 0$  too, and thus  $Y = 0$ , which is not the case. This accounts for one line of rank 2 matrices, and for these matrices,  $R(Y)$  is the set of vectors with first entry 0.

We can now limit our attention to matrices  $X(x, y, z)$  with  $z \neq 0$ , and to matrices  $Y(r, s, t)$  with  $s + t \neq 0$ . For these matrices, we see that the row spaces definitely contain some vectors with first entry nonzero, and so these row spaces are different from those that we have already considered.

There is one line of matrices  $X(x, y, z)$  where  $x = 0 = y$ , and since  $a \neq 0$ , we see that the matrices in this line have rank 2, and the corresponding row space is exactly the set of vectors with second entry 0. Similarly, there is one line of matrices  $Y(r, s, t)$  where  $r = 0 = s$ , and we see that these matrices have rank 2, and the corresponding row space is also the set of vectors with second entry 0.

Now consider matrices  $X = X(x, y, z)$  where  $z \neq 0$  and at least one of  $x$  or  $y$  is also nonzero. We argue that for such a matrix, the first and second columns must be linearly independent, and thus the rank is 2 or 3. The second column is nonzero in this case, and so if the first and second columns were dependent, the first column would be a scalar multiple of the second, and it would follow that  $z = 0$ , which is not the case. The first two columns of  $X$  are thus linearly independent, as claimed.

Now let  $Y = Y(r, s, t)$  where  $s + t \neq 0$  and at least one of  $r$  or  $s$  is also nonzero. We argue that the first and second columns of  $Y$  are linearly independent, and so  $Y$  has rank 2 or 3. Since the second column of  $Y$  is nonzero, we see that if the first two columns were dependent, then the first column would be a scalar multiple of the second, and this would force  $s + t = 0$ , which is not the case. The first two columns of  $Y$  are thus linearly independent, as claimed.

It suffices now to consider only matrices  $X \in S_a$  and  $Y \in T_a$  for which the first and second columns are linearly independent. Note that the row space of such a matrix necessarily contains vectors with first entry nonzero and vectors with second entry nonzero, and so the row spaces of these matrices are different from those that we considered previously.

If  $X = X(x, y, z)$  has rank 2 and its first two columns are linearly independent, then the third column must be a linear combination of the first two: say  $\alpha$  times the first column plus  $\beta$  times the second, where  $\alpha, \beta \in F$  are uniquely determined by  $X$ . It is clear that all matrices in the line of  $X$  determine the same pair  $(\alpha, \beta)$ , and we claim that this pair cannot arise from any other line of rank 2 matrices in  $S_a$ . To see why this is so, observe that we can write  $x = \alpha z$  and  $y = \alpha z + \beta x$ . It follows that given  $\alpha$  and  $\beta$ , the quantity  $z$  uniquely determines  $x$  and  $y$ , and so the line of  $X$  is determined, as claimed. Also, we see that the row space  $R(X)$  is the full space of vectors  $(r, s, t)$  such that  $t = \alpha r + \beta s$ . It is clear that this 2-dimensional space of row vectors uniquely determines  $\alpha$  and  $\beta$ . Then  $R(X)$  uniquely determines  $\alpha$  and  $\beta$ , and it follows that  $R(X)$  also determines the line

containing  $X$ .

Now suppose that  $Y = Y(r, s, t)$  has rank 2 and that its first two columns are independent. Then  $Y$  determines a pair  $(\alpha, \beta)$  of scalars such that the third column of  $Y$  is the corresponding linear combination of the first two. Then  $s = \beta r$  and  $t = \alpha r + \beta s$ , and so reasoning as before, we see that the pair  $(\alpha, \beta)$  arises from a unique line of rank 2 matrices in  $T_a$  and that the row space  $R(Y)$  uniquely determines the line containing  $Y$ .

Next, we show that if  $X = X(x, y, z)$  has rank 2 and its first two columns are linearly independent, then there exists a rank 2 matrix  $Y = Y(r, s, t)$  such that  $R(Y) = R(X)$ . If  $\alpha$  and  $\beta$  are determined by  $X$  as before, let  $w$  be the column vector with entries  $\alpha, \beta$  and  $-1$ . Then  $X \cdot w = 0$ , and in fact,  $R(X)$  is the space of row vectors  $v$  such that  $v \cdot w = 0$ .

If  $r, s, t \in F$  are arbitrary scalars, we have

$$0 = [r \ s \ t] \cdot X \cdot w = [x \ y \ z] \cdot Y \cdot w,$$

where  $Y = Y(r, s, t)$ . Since the row vector  $[x \ y \ z]$  is nonzero, it follows that not every column vector can be of the form  $Y \cdot w$  as  $Y$  runs over  $T_a$ , and so the map  $Y \mapsto Y \cdot c$  from  $T_a$  to the 3-dimensional space of column vectors is not surjective. This map, therefore, is also not injective, and thus there is some nonzero matrix  $Y = Y(r, s, t)$  such that  $Y \cdot w = 0$ . In particular, we conclude that  $Y$  has rank 2 and that  $R(Y)$  is exactly the space of row vectors  $v$  such that  $v \cdot w = 0$ . In other words,  $R(Y) = R(X)$ , as desired.

Finally, we observe that with no essential change, we can reverse the argument of the previous two paragraphs to prove that for each rank 2 matrix  $Y = Y(r, s, t)$ , where the first two columns are independent, there exists a rank 2 matrix  $X = X(x, y, z)$  such that  $R(X) = R(Y)$ . This completes the proof of the theorem. ■

**(3.2) THEOREM.** *Let  $0 \neq a \in F$ , where  $F$  is the field of order  $p$ , and let  $S_a$  be as above. Then  $k(G(S_a)) = p^6 + p^3 - 1 + n(p^2 - 1)(p - 1)$ , where  $n$  is the number of lines of rank 2 matrices in  $S_a$ .*

**Proof.** By Corollary 2.3, we know that  $k(G(S_a))$  is the sum of the quantities  $p^{3-e(v,X)}$ , where  $v$  runs over  $F^3$  and  $X$  runs over  $S_a$ , and where we recall that  $e(v, X)$  is the dimension of the subspace  $R(v) + R(X)$  of  $F^3$ . We have seen, however, that if we replace the row vector  $v = [r \ s \ t]$  by the matrix  $Y = Y(r, s, t) \in T_a$ , then  $R(v) = R(Y)$ . We need to compute, therefore, the dimensions  $d(X, Y)$  of the spaces of the form  $R(X) + R(Y)$  as  $(X, Y)$  runs over all  $p^6$  pairs of matrices  $X \in S_a$  and  $Y \in T_a$ . To compute  $k(G(S_a))$ , therefore, we then sum the numbers  $p^{3-d(X,Y)}$ .

If either  $X$  or  $Y$  has rank 3, then clearly,  $d(X, Y) = 3$ , and also,  $d(X, Y) = 3$  if both  $X$  and  $Y$  have rank 2, but they have different row spaces. Note that there are exactly  $n(p - 1)$  rank 2 matrices in  $S_a$  and by Theorem 3.1, there are also exactly  $n(p - 1)$  rank 2 matrices in  $T_a$ . We know that all other nonzero matrices in these spaces have rank 3.

Of course,  $d(0, 0) = 0$  and it follows by Theorem 3.1, that there are just three other ways that  $d(X, Y)$  can be different from 3. There are  $n(p - 1)$  pairs of the form  $(0, Y)$ , where  $Y \in T_a$  has rank 2; there are  $n(p - 1)$  pairs of the form  $(X, 0)$ , where  $X \in S_a$  has rank 2 and finally, there are  $n(p - 1)^2$  pairs of matrices  $(X, Y)$ , where  $X$  and  $Y$  are in corresponding lines of rank 2 matrices in  $S_a$  and  $T_a$ , respectively. In each of these three cases,  $d(X, Y) = 2$ , and we see that the total number of pairs  $(X, Y)$  such that  $d(X, Y) = 2$

is  $2n(p-1) + n(p-1)^2 = n(p^2-1)$ . The number of pairs where  $d(X, Y) = 3$ , therefore, is  $(p^6-1) - n(p^2-1)$ , and this yields

$$k(G(S_a)) = p^3 + n(p^2-1)p + (p^6-1) - n(p^2-1) = p^6 + p^3 - 1 + n(p^2-1)(p-1),$$

as claimed.  $\blacksquare$

To determine the number  $n$  that appears in Theorem 3.2, we must count the lines of rank 2 matrices in  $S_a$ . One such line consists of the matrices  $X(x, y, z)$  where  $z = 0 = x$ . For every other rank 2 matrix in  $S_a$ , we have  $z \neq 0$ , and so each line of rank 2 matrices other than the line where  $z = 0 = x$  contains a unique matrix  $X = X(x, y, z)$  with  $z = 1$ . Then  $\det(X) = x^3 + y^2 - ax - xy$ , and so  $X$  has rank 2 precisely when this determinant vanishes. If we write  $n_a$  to denote the number of ordered pairs  $(x, y)$  such that  $x^3 + y^2 = ax + xy$ , where  $x, y \in F$ , we see, therefore, there are exactly  $n_a + 1$  lines of rank 2 matrices in  $S_a$ .

Now given a prime  $p$ , write  $\Sigma(p) = |\{n_a \mid 0 \neq a \in F\}|$ . By Theorem 3.2, we see that as  $a$  varies among the nonzero elements of the field  $F$  of order  $p$ , the various groups  $G(S_a)$  have  $\Sigma(p)$  different numbers of conjugacy classes. All of these groups have order  $p^9$ , however, and so to prove Theorem A, it suffices to show that  $\Sigma(p) \rightarrow \infty$  as  $p \rightarrow \infty$ . We accomplish this in the next section by appealing to the theory of elliptic curves over finite fields.

#### 4. Elliptic curves.

Let  $E_a$  denote the curve  $x^3 + y^2 = ax + xy$  over the field  $F$  of prime order  $p > 2$ , where  $a \in F$ . The change of variables,  $X = -x, Y = y - x/2$ , yields the curve  $Y^2 = X(X^2 + X/4 - a)$ . If  $a$  is different from 0 and different from  $-1/64$ , the cubic in  $X$  has distinct roots, and so  $E_a$  is an elliptic curve, and we write  $\mathcal{E}(p)$  to denote this family of  $p-2$  curves. Adding a point at infinity produces the projective completion of  $E_a$ , and we note that the number of points defined over  $F$  on this projective curve is  $|E_a(F)| = n_a + 1$ , where  $n_a$  is as before. For the sake of completeness, note that if  $a = 0$ , then  $n_a = p-1$ , while if  $a = -1/64$ , then  $n_a = p-1$  if  $-2$  is a quadratic residue modulo  $p$ , and  $n_a = p+1$  otherwise.

We are interested in how  $|E_a(F)|$  varies for elliptic curves  $E_a$  in our family. Since  $\Sigma(p) \geq |\{|E_a(F)| \mid E_a \in \mathcal{E}(p)\}|$ , and it is our goal is to show that  $\Sigma(p)$  approaches infinity with  $p$ , we want to show that as  $a$  varies, the number of different values of  $|E_a(F)|$  approaches infinity with  $p$ .

Several theorems on the number of points on a general elliptic curve over  $F$  are available. By the theorem of Hasse-Weil [5], for example, the number of points on an elliptic curve over  $F$  is  $p + 1 - t$ , where

$$-2\sqrt{p} \leq t \leq 2\sqrt{p},$$

and results of Deuring give precise information about how often any particular number  $t$  arises. Specifically, we have the following.

**(4.1) THEOREM (Deuring [3], [6].)** *If  $t$  is an integer such that  $-2\sqrt{p} < t < 2\sqrt{p}$ , then the number of isomorphism classes of elliptic curves over  $F$  with exactly  $p + 1 - t$  points is  $H(t^2 - 4p)$ , where  $H(D)$  is the Kronecker class number of  $D$ .*

The relevant definition is this.

**DEFINITION.** Let  $D \in \mathbb{Z}$  be a negative integer congruent to 0 or 1 mod 4. The **Kronecker class number**  $H(D)$  is the cardinality of the set of  $SL(2, \mathbb{Z})$ -orbits of positive-definite binary quadratic forms  $aX^2 + bXY + cY^2$  with  $a, b, c \in \mathbb{Z}$  with discriminant  $b^2 - 4ac$  equal to  $D$ .

This is related to the class number  $h(d)$  of the field  $\mathbb{Q}[\sqrt{d}]$  by  $H(D) = \sum h(d)$ , where the sum runs over all negative integers  $d$  dividing  $D$ , such that  $D/d$  is a perfect square and  $d$  is congruent to 0 or 1 mod 4.

Now  $H(D) > 0$  for every negative integer congruent to 0 or 1 mod 4, and thus  $H(t^2 - 4p) > 0$  for all integers  $t$  with  $|t| < 2\sqrt{p}$ . It follows that if we look at all elliptic curves over  $F$ , and not just the curves in our family, the number of different numbers of points on these curves is  $1 + 2\lfloor\sqrt{p}\rfloor$ , which, of course, approaches infinity with  $p$ . We would be done, therefore, if every elliptic curve over  $F$  were isomorphic to some member of our family of curves.

Although it is not true that every isomorphism class of elliptic curve over  $F$  is represented by a curve in the family  $\mathcal{E}(p)$ , we can show, nevertheless, that our family is sufficiently well distributed among the isomorphism classes of for us to obtain the desired result. If  $a \neq 0, -1/64$ , it is easy to see that  $|E_a(F)|$  is even, and calculations for small primes  $p$  show that as  $a$  varies,  $|E_a(F)|$  takes on almost all (but not necessarily all) even integers of the form  $p + 1 - t$ , where  $|t| < 2\sqrt{p}$ .

First, we consider how often two curves in the family  $\mathcal{E}(p)$  can be isomorphic. If  $E_a$  and  $E_b$  are isomorphic over  $F$ , then they have the same  $j$ -invariant [5]. Since

$$j(E_a) = \frac{110592a^3 + 6912a^2 + 144a + 1}{64a^3 + a^2},$$

we see that at most three such curves can have any given  $j$ -invariant, and so the  $p - 2$  elliptic curves in  $\mathcal{E}(p)$  lie in at least  $(p - 2)/3$  different isomorphism classes. (A more careful calculation shows that there are approximately  $0.8p$  such classes.) The fact that  $\Sigma(p)$  approaches infinity with  $p$  will then follow by bounding  $H(t^2 - 4p)$  from above.

**(4.2) THEOREM.** *Given  $\delta > 0$ , there exists  $K > 0$  depending only on  $\delta$  such that*

$$H(D) < K(-D)^{0.5+\delta} \ln(-D)$$

for all negative integers  $D$  congruent to 0 or 1 mod 4.

**Proof.** One easily shows for negative integers  $d$  that

$$h(d) < \frac{1}{\pi} \sqrt{-d} \ln(-d).$$

(See [2], page 296.) In fact, the best bound known [1] is also a constant times  $\sqrt{-d} \ln(-d)$ , and computational evidence indicates that this is tight.

Now write  $-D = R^2Q$ , where  $Q$  is square-free, and note that the squares that divide  $-D$  are exactly the numbers  $r^2$ , where  $r|R$ . In the following computation, we write  $\sigma(R)$  to denote the sum of the positive divisors of  $R$ . We have

$$\begin{aligned} H(D) &\leq \sum_{r|R} h(D/r^2) < \frac{1}{\pi} \sum_{r|R} \frac{\sqrt{-D}}{r} (\ln(-D) - 2 \ln(r)) \\ &< \frac{\sqrt{-D} \ln(-D)}{\pi} \sum_{r|R} \frac{1}{r} \\ &= \frac{\sqrt{-D} \ln(-D) \sigma(R)}{\pi R} \\ &< K(-D)^{0.5+\delta} \ln(-D), \end{aligned}$$

for some number  $K$ . The last inequality follows because  $\sigma(R) = O(R^{1+\delta})$  for all  $\delta > 0$ . (See Theorem 322 of [4].) ■

In particular, if  $|t| < 2\sqrt{p}$ , it follows that  $H(t^2 - 4p) < K(4p)^{0.5+\delta} \ln(4p)$ , where  $\delta$  and  $K$  are as in Theorem 4.2.

The following completes the proof of Theorem A.

**(4.3) COROLLARY.**  $\Sigma(p) \rightarrow \infty$  as  $p \rightarrow \infty$ .

**Proof.** Fix  $\delta$  with  $0 < \delta < 0.5$ , choose  $K$  as in Theorem 4.2 and write  $B(p) = K(4p)^{0.5+\delta} \ln(4p)$ . If  $|t| < 2\sqrt{p}$ , we have  $H(t^2 - 4p) < B(p)$ , and by Deuring's theorem, therefore, the number of isomorphism classes of elliptic curves over  $F = \mathbb{Z}/p\mathbb{Z}$  that have exactly  $p+1-t$  points is at most  $B(p)$ . It follows that there are at most  $3B(p)$  curves  $E_a$  in the family  $\mathcal{E}(p)$  such that  $|E_a(F)| = p+1-t$ . Among the  $p-2$  curves in our family, therefore, the quantity  $|E_a(F)|$  takes on at least

$$\frac{p-2}{3B(p)} = \frac{p-2}{3K(4p)^{0.5+\delta} \ln(4p)}$$

different values. Since  $\delta < 0.5$ , this approaches infinity with  $p$ , and the proof is complete. ■

## REFERENCES

1. O. Bordellès, Explicit upper bounds for the average order of  $d_n(m)$  and application to class number, *J. Inequal. Pure Appl. Math.* **3** (2002), no. 3, Article 38, 15 pp. (electronic).
2. H. Cohen, *A course in computational algebraic number theory* GTM 138 Springer, Berlin 1993.
3. M. Deuring, “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper”, *Abh. Math. Sem. Hansischen Univ.* **14** (1941) 197–272.
4. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*. Clarendon Press, Oxford 1979.
5. J. Silverman, *The arithmetic of elliptic curves*. GTM 106 Springer, Berlin 1994.
6. W. Waterhouse, “Abelian varieties over finite fields”, *Ann. Sci. École Norm. Sup.* **2** (1969), 521–560.

### Address of authors:

Mathematics Department  
480 Lincoln Drive  
Madison WI 53706  
USA

boston@math.wisc.edu  
isaacs@math.wisc.edu