MATHEMATICS OF COMPUTATION
VOLUME 47, NUMBER 176
OCTOBER 1986, PAGES 741–747

Some Remarks on Cohen-Lenstra Heuristics

By Lawrence C. Washington

Abstract. Cohen and Lenstra have given a heuristic model which predicts the fraction of imaginary quadratic fields with class number divisible by a given odd prime p and of those whose class groups have a given p-rank. We show that these numbers also arise by considering the proportion of matrices in $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ with 1 as an eigenvalue and those whose 1-eigenspaces have a given dimension, then letting $n \to \infty$. In the last section we discuss some relations with elliptic curves.

In a recent paper, H. Cohen and H. Lenstra [1] give a heuristic model which predicts that for an odd prime p the proportion of imaginary quadratic fields with class number divisible by p should be

$$1 - \prod_{n=1}^{\infty} (1 - p^{-n}),$$

and the proportion whose class groups have p-rank r should be

$$p^{-r^2} \prod_{n=1}^{\infty} (1 - p^{-n}) \prod_{k=1}^{r} (1 - p^{-k})^{-2}.$$

For example, the proportion with class number divisible by 3 should be .43987, which agrees rather well with numerical data.

In the present paper, we show that the above numbers arise in another way, which at present does not seem to have a direct connection with class groups; but if it did, perhaps via some geometric interpretation, it might be possible to make progress towards proofs of the above heuristics.

THEOREM 1. (a) *Consider the proportion of matrices in* $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ *which have* 1 *as an eigenvalue. As* $n \to \infty$, *this proportion has the limit*

$$1 - \prod_{n=1}^{\infty} (1 - p^{-n}).$$

(b) *Let* $r \geqslant 1$ *and consider the proportion of matrices whose* 1*-eigenspaces have dimension exactly* r. *The limit of this proportion as* $n \to \infty$ *is*

$$p^{-r^2} \prod_{n=1}^{\infty} (1 - p^{-n}) \prod_{k=1}^{r} (1 - p^{-k})^{-2}.$$

In the last section of the paper we discuss how these results relate to elliptic curves.

Received August 13, 1985.
1980 *Mathematics Subject Classification*. Primary 12A25; Secondary 15A18, 14K07.

0025-5718/86 $1.00 + $.25 per page

1. Proof of Theorem 1. Let $n \geqslant r \geqslant 1$. We count the number M_r^n of matrices in $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ whose 1-eigenspaces have dimension at least r. The idea is to count for each r-dimensional subspace the number of matrices which act as the identity on that subspace. But a matrix with 1 as an eigenvalue of multiplicity $r+1$ gets counted more than once, so we subtract off such matrices and recount them. Similarly, we adjust for those with 1 as an eigenvalue of multiplicity $r+2$, etc. More precisely, let S_i^j denote the number of i-dimensional subspaces of $(\mathbf{Z}/p\mathbf{Z})^j$. It is easy to see that

$$S_i^j = \frac{(p^j-1)(p^j-p)\cdots(p^j-p^{i-1})}{(p^i-1)(p^i-p)\cdots(p^i-p^{i-1})} = \frac{(p^j-1)(p^{j-1}-1)\cdots(p^{j-i+1}-1)}{(p^i-1)(p^{i-1}-1)\cdots(p-1)}$$

(the numerator comes from choosing a basis of i independent vectors; the denominator is the order of GL_i, which operates transitively on the possible bases of a given subspace). Observe that $S_i^j = S_{j-i}^j$. Considering for example the i-dimensional subspace of $(\mathbf{Z}/p\mathbf{Z})^j$ spanned by the first i standard basis vectors, we find that the number of matrices in GL_j acting as the identity on a given i-dimensional subspace is

$$I_i^j = p^{i(j-i)}|\mathrm{GL}_{j-i}| = (p^j-p^i)(p^j-p^{i+1})\cdots(p^j-p^{j-1}).$$

Let $X_0^r = 1$, and for $j \geqslant 1$, let

$$X_j^r = 1 - \sum_{i=0}^{j-1} S_{r+i}^{r+j} X_i^r;$$

then

$$M_r^n = \sum_{i=0}^{n-r} S_{r+i}^n I_{r+i}^n X_i^r.$$

This is just the inclusion-exclusion type argument mentioned above. To see what is happening, consider a matrix which has 1 as an eigenvalue of multiplicity exactly $r+2$. This matrix gets counted S_r^{r+2} times by the factor S_r^n, S_{r+1}^{r+2} times by S_{r+1}^n, and $S_{r+2}^{r+2} = 1$ time by S_{r+2}^n. It does not get counted past this term. The total count for this matrix is therefore

$$S_r^{r+2}X_0^r + S_{r+1}^{r+2}X_1^r + S_{r+2}^{r+2}X_2^r = (1 - X_2^r) + X_2^r = 1.$$

In this way we see that each matrix gets counted exactly once, as desired.

LEMMA.

$$X_j^r = p^{j(j+1)/2}\frac{(1-p^r)(1-p^{r+1})\cdots(1-p^{r+j-1})}{(p-1)(p^2-1)\cdots(p^j-1)}.$$

Proof. The case $j = 0$ is trivially true. Assume the lemma is true up through $j-1$. We must show that

$$0 = 1 - \sum_{i=0}^{j-1} S_{r+i}^{r+j} X_i^r - p^{j(j+1)/2}\frac{(1-p^r)\cdots(1-p^{r+j-1})}{(p-1)\cdots(p^j-1)}.$$

Since $S_{r+i}^{r+j} = S_{j-i}^{r+j}$, this becomes

$$0 = 1 - \sum_{i=0}^{j} \frac{(p^{r+j}-1)\cdots(p^{r+i+1}-1)}{(p^{j-i}-1)\cdots(p-1)} p^{i(i+1)/2} \frac{(1-p^r)\cdots(1-p^{r+i-1})}{(p-1)\cdots(p^i-1)}.$$

Replace p^r by Y to get a polynomial

$$Q(Y) = 1 - \sum_{i=0}^{j} \frac{(p^jY-1)\cdots(p^{i+1}Y-1)}{(p^{j-i}-1)\cdots(p-1)} p^{i(i+1)/2} \frac{(1-Y)\cdots(1-p^{i-1}Y)}{(p-1)\cdots(p^i-1)}.$$

Let $0 \leqslant i \leqslant j$ and let $Y = p^{-i}$; then all terms vanish except 1 and the term indexed by i. It follows easily that $Q(p^{-i}) = 0$, so $Q(Y)$ has $j+1$ zeros. Since it has degree at most j, it vanishes identically. Therefore $Q(p^r) = 0$, as desired.

We are interested in the ratio $M_r^n/|\mathrm{GL}_n|$. Putting together the lemma and the above expression for M_r^n, we obtain

$$\frac{M_r^n}{|\mathrm{GL}_n|} = \sum_{i=0}^{n-r} \frac{S_{r+i}^n I_{r+i}^n X_i^r}{|\mathrm{GL}_n|}$$

$$= \sum_{i=0}^{n-r} \frac{p^{i(i+1)/2}(1-p^r)\cdots(1-p^{r+i-1})}{(p^{r+i}-1)\cdots(p^{r+i}-p^{r+i-1})(p-1)\cdots(p^i-1)}.$$

Let $r = 1$. We obtain the following.

THEOREM 2. *The proportion of matrices in* $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ *having* 1 *as an eigenvalue is*

$$\frac{1}{p-1} - \frac{1}{(p-1)(p^2-1)} + \cdots + \frac{(-1)^{n-1}}{(p-1)\cdots(p^n-1)}.$$

The proof of part (a) of Theorem 1 is now easy to obtain. We start with the identity

$$(1+aX)(1+aX^3)(1+aX^5)\cdots$$

$$= 1 + \frac{aX}{1-X^2} + \frac{a^2X^4}{(1-X^2)(1-X^4)} + \frac{a^3X^9}{(1-X^2)(1-X^4)(1-X^6)} + \cdots$$

(see [2, Formula 19.5.1]). Let $a = -X$ and then $Y = X^2$ to obtain

$$(1-Y)(1-Y^2)(1-Y^3)\cdots$$

$$= 1 - \frac{Y}{1-Y} + \cdots + \frac{(-1)^jY^{j(j+1)/2}}{(1-Y)\cdots(1-Y^j)} + \cdots.$$

Let $Y = p^{-1}$. We find that

$$1 - \prod_{j=1}^{\infty}(1-p^{-j}) = \frac{p^{-1}}{1-p^{-1}} - \frac{p^{-3}}{(1-p^{-1})(1-p^{-2})} + \cdots,$$

which is the limit of the expression in Theorem 2. This proves part (a).

Now consider $r \geqslant 1$. The proposition with 1 as an eigenvalue of multiplicity exactly r is (write $r + i = (r + 1) + (i - 1)$)

$$\frac{M_r^n - M_{r+1}^n}{|\mathrm{GL}_n|} = \frac{S_r^n I_r^n}{|\mathrm{GL}_n|} + \sum_{i=1}^{n-r} \frac{S_{r+i}^n I_{r+i}^n X_i^r - S_{r+i}^n I_{r+i}^n X_{i-1}^{r+1}}{|\mathrm{GL}_n|}$$

$$= \frac{1}{(p^r - 1)\cdots(p^r - p^{r-1})}$$

$$+ \sum_{i=1}^{n-r} \frac{p^{i(i-1)/2}(1 - p^{r+1})\cdots(1 - p^{r+i-1})}{(p^{r+i} - 1)\cdots(p^{r+i} - p^{r+i-1})(p - 1)\cdots(p^{i-1} - 1)} \frac{(1 - p^{i+r})}{(p^i - 1)}$$

$$= \frac{p^{(r-r^2)/2}}{(p^r - 1)\cdots(p - 1)}\left(1 + \sum_{i=1}^{n-r} \frac{(-1)^i p^{-ri}}{(p - 1)\cdots(p^i - 1)}\right)$$

$$= \frac{p^{-r^2}}{(1 - p^{-r})\cdots(1 - p^{-1})}\left(1 + \sum_{i=1}^{n-r} \frac{(-1)^i p^{-ri - i(i+1)/2}}{(1 - p^{-1})\cdots(1 - p^{-i})}\right).$$

In the identity used above in the proof of part (a), let $a = -X^{2r+1}$ and $Y = X^2$ to obtain

$$(1 - Y^{r+1})(1 - Y^{r+2})\cdots = 1 - \frac{Y^{r+1}}{1 - Y} + \cdots + \frac{(-1)^j Y^{rj + j(j+1)/2}}{(1 - Y)\cdots(1 - Y^j)} + \cdots.$$

Letting $Y = p^{-1}$, we obtain

$$\lim_{n\to\infty} \frac{M_r^n - M_{r+1}^n}{|\mathrm{GL}_n|} = \frac{p^{-r^2}}{(1 - p^{-r})\cdots(1 - p^{-1})}(1 - p^{-r-1})(1 - p^{-r-2})\cdots$$

$$= p^{-r^2} \prod_{j=1}^{\infty}(1 - p^{-j}) \prod_{k=1}^{\infty}(1 - p^{-k})^{-2},$$

which is part (b) of Theorem 1.

2. Elliptic Curves. Let E be an elliptic curve defined over $\mathbf{Q}$ without complex multiplication and consider the extension of $\mathbf{Q}$ obtained by adjoining, for a prime p, the coordinates of the points of p-power order of E. A theorem of Serre [3] states that for all but finitely many p the Galois group of this extension is isomorphic to $\mathrm{GL}_2(\mathbf{Z}_p)$, where $\mathbf{Z}_p$ denotes the p-adic integers. It follows for such p that the points of order p^n yield the Galois group $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$, which acts as follows: Choose a basis for the points of order p^n. Then vectors in $(\mathbf{Z}/p^n\mathbf{Z})^2$ represent points of order p^n, and a matrix in GL_2 acts in the usual way on these vectors.

Let l be a prime for which E has good reduction. If $E \bmod l$ has a point of order p defined over $\mathbf{Z}/l\mathbf{Z}$, then the Frobenius element (actually a conjugacy class) for l fixes the corresponding global point of order p. Therefore, the matrix corresponding to the Frobenius has 1 as an eigenvalue. By the Chebotarev Density Theorem, the density of those l for which there is a point of order p is just the proportion of matrices with 1 as an eigenvalue. From Theorem 2, this is

$$\frac{1}{p - 1} - \frac{1}{(p - 1)(p^2 - 1)} = \frac{p^2 - 2}{(p - 1)(p^2 - 1)}.$$

We note in passing that the case of an extension with group $\mathrm{GL}_1(\mathbf{Z}_p) \simeq \mathbf{Z}_p^\times$ also arises naturally by adjoining all p-power roots of unity to $\mathbf{Q}$ (perhaps this should be considered as adjoining the points of p-power order of the multiplicative group G_m). The field $\mathbf{F}_l$ has a pth root of unity if and only if the Frobenius for l, namely the 1 by 1 matrix (l), has 1 as an eigenvalue mod p, which happens if and only if $l \equiv 1 \bmod p$. The density of such l is $1/(p-1)$, as predicted by Theorem 2.

If there exists a geometric object whose points of order p correspond in a similar way to the limit as $n \to \infty$ of $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$, and which relates to the class groups of imaginary quadratic fields, then it might be possible to use Theorem 1 to prove some of the heuristic estimates of Cohen-Lenstra. But it is not clear where to look for such an object. It seems that abelian varieties will not work since they tend to give proper subgroups of $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$ as Galois groups.

We now return to the case of elliptic curves in order to point out an ever-present problem with heuristic arguments. In the Cohen-Lenstra model for class groups of imaginary quadratic fields, a group G is given weight $1/|\mathrm{Aut}(G)|$, and the frequency with which it occurs is supposed to be its weight divided by the sum of the weights of all groups under consideration. Suppose we apply this to an elliptic curve E as above to see how often $E \bmod l$ has a given p-group for its group of points of p-power order. The possible groups and the size of their automorphism groups are as follows ((n) denotes the cyclic group of order n).

The group (1) has one automorphism.

The group (p^n) has $\phi(p^n)$ automorphisms, so receives weight $1/\phi(p^n)$.

The group $(p^n) \times (p^n)$ has automorphism group $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$. Using the exact sequence

$$1 \to 1 + pM_2(\mathbf{Z}/p^n\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \to 1,$$

we find that $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$ has order $p^{4n-4}(p^2-1)(p^2-p)$.

Writing elements of $(p^n) \times (p^m)$ as ordered pairs, we find that the automorphisms are given by $(1,0) \mapsto (a,b)$ with $p \nmid a$, $(0,1) \mapsto (c,d)$ with $p \nmid d$ and $p^m c = 0$. Therefore, there are $\phi(p^n)\phi(p^m)p^{2m}$ automorphisms.

The sum W of the weights is easily found by summing appropriate geometric series to obtain

$$W = 1 + \frac{p(p^4 - 2p^2 + p + 1)}{(p-1)^4(p+1)^2} = \frac{p^6 - p^5 - p^4 + 2p^3 - p + 1}{p^6 - 2p^5 - p^4 + 4p^3 - p^2 - 2p + 1}.$$

The heuristic probability that p divides the order of E_l is then

$$\frac{W-1}{W} = \frac{p(p^4 - 2p^2 + p + 1)}{p^6 - p^5 - p^4 + 2p^3 - p + 1} = p^{-1} + p^{-2} - p^{-5} - p^{-7} + \cdots.$$

For $p = 3$ this yields $201/457 \approx .4398$, which is slightly more than the correct value $7/16 = .4375$. Of course, there are problems with the above heuristic model. Besides the fact that it gives the wrong answer, it also mandates, without any apparent reason, that the rank is at most 2. However, it could be considered as a reasonable attempt. Now, how can one judge heuristic models? First of all, there needs to be a "reasonable" model. Secondly, the predicted results must agree with the numerical data. The above heuristic could be regarded as fulfilling, to some

extent, both requirements, especially since it would take an enormous amount of computation to distinguish empirically between .4398 and .4375. So it easily could be the case that the above heuristic model for elliptic curves could be accepted as valid, even though it is false.

Finally, we present some results which indicate that there is possibly a modification of the Cohen-Lenstra idea which works for elliptic curves. We calculate how often each possible p-group actually occurs, still under the assumption that the p-power points yield the Galois group $\mathrm{GL}_2(\mathbf{Z}_p)$.

We first consider $(p^n) \times (p^n)$ with $n \geq 1$. Suppose $M \in \mathrm{GL}_2(\mathbf{Z}_p)$ represents the Frobenius for l. Then $M \equiv I \bmod p^n$, so $M = I + p^n N$. It is easy to see that we get $(p^n) \times (p^n)$ for the exact p-part of E_l if and only if N does not have 0 as an eigenvalue mod p, so $\det N \not\equiv 0 \bmod p$. Working mod p^{n+1}, we find that there are $(p^2 - 1)(p^2 - p)$ choices for $N \bmod p$, hence this many choices for M. Since $\mathrm{GL}_2(\mathbf{Z}/p^{n+1}\mathbf{Z})$ has order $p^{4n}(p^2 - 1)(p^2 - p)$, the density of such M, hence the density of $(p^n) \times (p^n)$, is p^{-4n}.

Now fix $n > m \geq 1$, and consider collectively the groups of the form $(p^k) \times (p^m)$ with $k \geq n$. Let M again represent the Frobenius. Then $M = I + p^m N$ with $N \not\equiv 0 \bmod p$. There is a vector $v \not\equiv 0 \bmod p$ such that $Mv \equiv v \bmod p^n$. This implies that $Nv \equiv 0 \bmod p^{n-m}$. Then N is conjugate to a matrix of the form $\left(\begin{smallmatrix} 0 & x \\ 0 & y \end{smallmatrix}\right)$ with not both x, y zero mod p. If $y \not\equiv 0 \bmod p$, this is conjugate to $\left(\begin{smallmatrix} 0 & 0 \\ 0 & y \end{smallmatrix}\right)$. The centralizer of $\left(\begin{smallmatrix} 0 & 0 \\ 0 & y \end{smallmatrix}\right)$ is the group of all invertible diagonal matrices. We work with $M \bmod p^n$, hence with $N \bmod p^{n-m}$, so the centralizer of N has order $\phi(p^{n-m})^2$. Therefore, taking into account the $\phi(p^{n-m})$ choices for y, we find $|G_{n-m}|/\phi(p^{n-m})$ matrices M in this case. The centralizer of $\left(\begin{smallmatrix} 0 & 1 \\ 0 & y \end{smallmatrix}\right)$, $y \equiv 0 \bmod p$, is the group of matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & a+by \end{smallmatrix}\right)$, which has order $\phi(p^{n-m})p^{n-m}$. There are p^{n-m-1} choices for y, so we get $|G_{n-m}|/p\phi(p^{n-m})$ matrices M. Adding the two cases together and dividing by $|G_n|$, we obtain the density $(p + 1)/(p - 1)p^{n+3m}$. It follows that the probability of obtaining exactly $(p^n) \times (p^m)$, $n > m \geq 1$, is

$$\frac{p+1}{p} \frac{1}{p^{n+3m}}.$$

Finally, fix n and consider collectively the groups (p^a) with $a \geq n$. The matrix M is conjugate to a matrix congruent to $\left(\begin{smallmatrix} 1 & b \\ 0 & d \end{smallmatrix}\right) \bmod p^n$. Suppose $d \not\equiv 1 \bmod p$. Then we can obtain the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \bmod p^n$. If $d \equiv 1 \bmod p$ then $b \not\equiv 0 \bmod p$; otherwise $M \equiv I \bmod p$ and E_l contains $(p) \times (p)$. Conjugation by $\left(\begin{smallmatrix} b^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ now yields $\left(\begin{smallmatrix} 1 & 1 \\ 0 & d \end{smallmatrix}\right)$. The centralizer of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, $d \not\equiv 1 \bmod p$, is the group of invertible diagonal matrices mod p^n, which has order $\phi(p^n)^2$. The centralizer of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & d \end{smallmatrix}\right)$, $d \equiv 1 \bmod p$, is the group of matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & a+bd-b \end{smallmatrix}\right)$, which has order $\phi(p^n)p^n$. The combined density for these two cases is easily calculated to be $(p^2 - p - 1)/(p - 1)^2 p^n$. Therefore the density for the group (p^n) is

$$\frac{p^2 - p - 1}{(p-1)p^{n+1}}.$$

The heuristic model is seen to predict densities for the cyclic groups (p^n) slightly higher than the actual values and, correspondingly, it predicts slightly lower densities than the actual values for the noncyclic groups. More precisely, if W is as above,

then (p^n) has predicted density and actual density

$$\frac{p}{p-1}\frac{1}{W}\frac{1}{p^n} \quad \text{and} \quad \frac{p^2-p-1}{p(p-1)}\frac{1}{p^n},$$

respectively. For $p = 3$, we have $.840/3^n$ and $.833/3^n$. For $(p^n) \times (p^n)$, the predicted and actual densities are

$$\frac{p^3}{(p^2-1)(p-1)}\frac{1}{W}\frac{1}{p^{4n}} \quad \text{and} \quad \frac{1}{p^{4n}}.$$

For $p = 3$, these become $.945/3^{4n}$ and $1/3^{4n}$. For $(p^n) \times (p^m)$, the values are

$$\frac{p^2}{(p-1)^2}\frac{1}{W}\frac{1}{p^{n+3m}} \quad \text{and} \quad \frac{p+1}{p}\frac{1}{p^{n+3m}}.$$

For $p = 3$, these are $1.260/3^{n+3m}$ and $1.333/3^{n+3m}$.

Note that the ratio between the actual and predicted densities is the same, namely $p^3/(p^2-1)(p-1)W$, in both noncyclic cases. The significance of this is not clear, but perhaps it indicates that there is a heuristic model based on some modification of the Cohen-Lenstra technique which will yield the correct densities.

Acknowledgment. The author would like to thank Ken Ribet for some helpful conversations.

Department of Mathematics
University of Maryland
College Park, Maryland 20742

1. H. COHEN & H. W. LENSTRA, JR., "Heuristics on class groups of number fields," *Number Theory Noordwijkerhout*. 1983 (H. Jager, ed.), Lecture Notes in Math., vol. 1068, Springer-Verlag, Berlin and New York, 1984, pp. 33–62.

2. G. H. HARDY & E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, London, 1968.

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