

## POSSIBLE PROBLEMS

Some possible problems are outlined below. One should note that each of the following subsections contains a description of a general problem and in some cases two to three possible avenues for research related to the general problem. Thus it is possible that more than one team will work in the area described by one of the following subsections. These teams would, of course, be working on different aspects of the general problem described. This is especially true of subsections I, III and IV.

**I. Average Frobenius Distributions.** A topic of central importance in number theory over the past decade has been the theory of elliptic curves. We can think of an elliptic curve as the set of fractional solutions to an equation of the form

$$(1) \quad E : y^2 = x^3 + Ax + B.$$

One of the major conjectures in this area is the Lang-Trotter conjecture (see [10]). This conjecture deals with the *local* behavior of a given curve, that is the number of solutions to an equation like the one above modulo a prime  $p$ . It is known that the number of solutions to such an equation modulo  $p$  counting a point at infinity is between  $p+1-2\sqrt{p}$  and  $p+1+2\sqrt{p}$ , and that all integers in this range are obtained by some curve modulo  $p$ . Thus, given an elliptic curve  $E$  as above, it is quite natural to let  $a_E(p) = p + 1 - \#E(\mathbb{F}_p)$ , where  $\#E(\mathbb{F}_p)$  denotes the number of solutions to our equation plus 1 to account for the point at infinity. Then we are interested in determining how often  $a_E(p)$  takes on a given value as the prime  $p$  varies. For instance, we may notice that if we consider the curve  $E : y^2 = x^3 + 1$ , then  $a_E(11) = 0$ . This is because when we count solutions to  $y^2 = x^3 + 1$  modulo 11, we find that there are 11 and when we add 1 for the point at infinity, we see that  $\#E(\mathbb{F}_p) = 12$  which is  $p + 1$  in this case. Now, the question that we are interested in answering in this context becomes: ‘As we let  $p$  vary over all primes, how often do we have  $a_E(p) = 0$ ?’

The Lang-Trotter conjecture asserts that if  $n$  is any integer and if  $E$  is an elliptic curve, then as we let  $p$  vary over all primes up to some bound  $X$  the number of times that we have  $a_E(p) = n$  should grow like a constant times  $\sqrt{X}/\log X$ , where the constant depends only on  $E$  and  $n$ . This conjecture has been shown to be true in an average sense (see [6], [5]). However, based on some recent computations [8] and additional averaging theorems [9], there remains some doubt as to whether the conjecture holds for all curves. One readily attackable computational problem is to gather more computational evidence to help us better understand this conjecture. The PI has already done some computations related to this problem and could get students started gathering more data right away. In addition, students could study other algorithms for computing the  $a_E(p)$ ’s and implement these to obtain quicker code. This would allow us to greatly increase the computational data related to this problem and hopefully shed more light on this mysterious conjecture.

In a slightly different direction, students could be introduced to counting techniques which have been used by the PI and others ([6],[5] and [9]) to prove that some variations of the Lang-Trotter conjecture are true when one averages over certain families of curves. In particular,

students could study the family of elliptic curves with a point of order 5 or the family of curves with a point of order 7 and try to show that something like the Lang-Trotter conjecture holds on average for this family of curves.

**II. The distribution of the partition function modulo a prime.** Given a number  $n$  a partition of  $n$  is a non-increasing sequence of numbers whose sum is  $n$ . For instance  $3, 1, 1$  is a partition of 5. We define  $p(n)$  to be the number of such partitions of  $n$ . For instance, a complete list of partitions of 4 is given by

$$(2) \quad \begin{array}{l} 1, 1, 1, 1 \\ 2, 1, 1 \\ 2, 2 \\ 3, 1 \\ 4 \end{array}$$

Thus  $p(4) = 5$ . One question that has received much attention lately is how the partition function is distributed modulo a given integer  $m$  (see [11] and references therein). For instance, we don't know how often  $p(n)$  is congruent to 3 modulo 11 as  $n$  varies.

This question is readily attackable from a computational standpoint. Students could begin to investigate these distributions right away. Also, the PI and co-PI have recently developed algorithms that should allow the quick computation of the generating function for  $p(n)$  modulo a prime  $p$ . Thus, one should be able to obtain many values of the partition function modulo various primes. The students could implement these algorithms as well as modify them to quickly compute many values of  $p(n)$  and study the distribution of this function modulo small primes. Hopefully, enough data could be gathered to make reasonable conjectures about the behavior of this function.

**III. Class Number Formulas.** For our purposes, a binary quadratic form is a homogeneous quadratic polynomial with integer coefficients; that is a polynomial of the form

$$(3) \quad f = ax^2 + bxy + cy^2,$$

where  $a, b, c \in \mathbb{Z}$ . The discriminant of the above form is given by  $d = b^2 - 4ac$ . Two such forms  $f(X)$  and  $g(X)$  (here  $X = (x_1, x_2)^T$ ) are said to be equivalent if there is an integral  $2 \times 2$  matrix of determinant  $\pm 1$  such that  $f(TX) = g(X)$ . One can show that any two equivalent forms have the same discriminant. So, it is quite natural to count the number of equivalence classes of binary quadratic forms of a given discriminant. We denote this number by  $H(d)$ .

If  $p$  is any prime then there is an amazing formula due to Kronecker which relates the values of  $H(k^2 - 4p)$  as  $k$  varies over the finite set of integers for which  $k^2 - 4p < 0$ . We

share this amazing formula below.

$$(4) \quad \sum_{k^2 \leq 4p} H(k^2 - 4p) = \begin{cases} 2p & \text{if } p \equiv 11 \pmod{12}. \\ 2p + 4 & \text{if } p \equiv 7 \pmod{12}. \\ 2p + 2 & \text{if } p \equiv 5 \pmod{12}. \\ 2p + 6 & \text{if } p \equiv 1 \pmod{12}. \end{cases}$$

The PI recently discovered the following related class number formula while studying elliptic curves with 3 torsion. For  $p \equiv 2 \pmod{3}$  a prime we have

$$(5) \quad \sum_{k^2 \leq 4p/9} H(9k^2 - 4p) = p - 1$$

Studies of elliptic curves with other prescribed torsion subgroups should yield similar class number formulas. However, in some cases the ideas used by the PI in the proof of the above formula become more difficult to implement. In any case, a computational study of curves with a given torsion subgroup should at least lead to an interesting conjecture for new class number formulas like the one above.

**IV. Eigenstructure of recursively defined matrices.** In enumeration problems, especially those arising in statistical mechanics, it is frequently desirable to understand the eigenstructure of recursively defined matrices. For example, when counting the number of configurations of non-attacking kings on a board of size  $n \times k$ , one is led to consider the  $k^{\text{th}}$  power of the matrix  $A_n$ , where  $A_n$  is defined recursively by

$$A_0 = (1), \quad A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$A_n = \begin{pmatrix} A_{n-1} & A_{n-2} \\ A_{n-1} & 0 \end{pmatrix}$$

in which the blocks  $A_{n-1}$ ,  $A_{n-2}$  are of different sizes, and the empty part of the matrix is padded with zeros.

If we knew the growth rate of the largest eigenvalue of  $A_n$  then we would be able to compute the asymptotics of the number of configurations: if we knew exact expressions for the eigenvalues, we could compute an exact expression.

It is easy to show that the largest eigenvalue  $\lambda_n$  of  $A_n$  satisfies  $\lambda_n^{1/n} \rightarrow \eta$  as  $n \rightarrow \infty$ , so that  $\lambda_n$  grows roughly like  $\eta^n$ . This gives an approximate recursion for  $\lambda_n$ :

$$\lambda_n \simeq \eta \lambda_{n-1}.$$

Now since  $A_n$  satisfies an exact recursion, and  $\lambda_n$  satisfies an approximate recursion, it is natural to ask about the structure of the Frobenius eigenvector, that is, the eigenvector  $\underline{e}_n$  corresponding to  $\lambda_n$ .

Numerical experiments suggest that there is indeed a recursive structure to  $\underline{e}_n$ : in fact, it appears that  $\underline{e}_n$  is very close (within about 1% of the largest co-ordinate) to being a scaled

concatenation of the vectors  $\underline{e}_{n-1}$  and  $\underline{e}_{n-2}$ . Moreover the error in this approximation also appears to be similarly recursive.

Students studying this phenomenon will be encouraged to study this and similar recursively defined matrices, to attempt to determine

- Whether this phenomenon can be analyzed fully
- How the phenomenon depends on the choice of recurrence
- Whether the phenomenon extends to other eigenvectors, for example, to the eigenvector corresponding to the second largest eigenvalue

There has been a lot of activity in the subject of eigenvalues of *random* matrices recently (see for example [2],[1]), with many applications to statistical mechanics, combinatorics and number theory: in particular, for many classes of random matrices having only real eigenvalues, the distributions of eigenvalues can be shown to converge to the Wigner distribution. Given this, it would also be of interest to numerically study the distribution of matrices such as  $A_n$ , to see what (if any) the limiting distribution of eigenvalues is.

**V. Fast algorithms for multiplying patterned matrices and other objects.** There are several well known algorithms for multiplying polynomials (for example, Fast Fourier transforms [3], Karatsuba's algorithm [7], etc.) and for multiplying matrices (Strassen's algorithm [12], Coppersmith and Winograd [4], etc.) which are significantly faster than naive methods, but rely on the use of more complicated recursions and also, on being able to use a larger set of constants. For example, multiplication of polynomials of degree less than  $n$  is easily seen to be  $O(n^2)$  by the naive method,  $O(n^{\log_2 3})$  if subtraction is allowed, as in Karatsuba's algorithm, and  $O(n \log n)$  if complex  $2^n$ th roots of unity are allowed. Similarly, Strassen's recursive algorithm using subtraction reduces the complexity of multiplying two  $n \times n$  matrices from  $O(n^3)$  to  $O(n^{\log_2 7})$ .

However, these algorithms often fail to be improvements over naive algorithms when the objects concerned are very sparse and highly patterned: such matrices often occur in studying discretizations of differential equations, for example. In this project, students will be encouraged to investigate Karatsuba, Strassen and FFT-type algorithms for sparse and patterned objects.

#### REFERENCES

- [1] Neil J. Calkin, C. Merino, S. Noble and M. Noy, *Improved Bounds for the Number of Forests and Acyclic Orientations in the Square Lattice*, (in preparation).
- [2] Neil J. Calkin and Herbert S. Wilf, *The Number of Independent Sets in a Grid Graph*, *SIAM Journal of Discrete Math*, **11** (1998), Number 1, 54–60.
- [3] P. Chiu, *Transforms, finite fields, and fast multiplication*, *Math. Mag.* **63** (1990), no. 5, 330–336.
- [4] D. Coppersmith, S. Winograd, *Matrix multiplication via arithmetic progressions*. *J. Symbolic Comput.* **9** (1990), no. 3, 251–280.
- [5] C. David and F. Pappalardi *Average Frobenius distributions of elliptic curves*. *Internat. Math. Res. Notices* 1999, no. 4, 165–183.
- [6] E. Fouvry and M. R. Murty, *On the distribution of supersingular primes*. *Canad. J. Math.* **48** (1996), no. 1, 81–104.

- [7] von zur Gathen, Joachim(D-PDRB); Gerhard, Jürgen(D-PDRB) Modern computer algebra.
- [8] K. James, C. Mehta and V. K. Murty, *Frobenius distributions and Galois representations – numerical evidence*, (preprint).
- [9] K. James, *Average Frobenius distributions of elliptic curves with 3-torsion*, (preprint).
- [10] S. Lang and H. Trotter, *Frobenius distributions in  $GL_2$ -extensions*. Distribution of Frobenius automorphisms in  $GL_2$ -extensions of the rational numbers. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976.
- [11] K. Ono, *Distribution of the partition function modulo  $m$* . Ann. of Math. (2) 151 (2000), no. 1, 293–307.
- [12] Strassen, V. Relative bilinear complexity and matrix multiplication. J. Reine Angew. Math. 375/376 (1987).
- [13] R. Weaver, *New congruences for the partition function*. Ramanujan J. 5 (2001), no. 1, 53–63.