POTENTIAL PROBLEM DESCRIPTIONS

I. Combinatorics

(a) Problem 1: Partitions

We define a partition of a number, n, to be a sequence of non-increasing positive integers that sum to n. We want to examine the number of partitions of n into powers of 2, in which no term is repeated more than twice. To accomplish this we can use the generating function $b(x) = \prod_{j=0}^{\infty}(1 + x^{2^j} + x^{2^{j+1}})$. Define $b_k = [x^k]b(x)$. Using $b(x)$, we find the following recursion relations $b_{2n} = b_n + b_{n-1}$ and $b_{2n+1} = b_n$. So, we have the sequence

$$1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, 4, 7, \ldots.$$

We will next show how we can use these coefficients to prove that $\mathbb{Q}^+$ is countable. Label a complete binary tree as follows. Define the root node to be $\frac{1}{1}$. Then for a parent node, $\frac{a}{b}$, we define the children to be $\frac{a}{a+b}$ and $\frac{a+b}{b}$. The binary tree with labels defined in this way is the Calkin-Wilf Tree. Reading the entries from the tree we can list all of the positive rational numbers, thus proving that $\mathbb{Q}^+$ is countable. In fact, these numbers are $\frac{b_0}{b_1}, \frac{b_1}{b_2}, \frac{b_2}{b_3}, \frac{b_3}{b_4}, \ldots$.
There are several open problems we can explore using the sequence $\{b_n\}$ and the Calkin-Wilf Tree. Can we prove that every third term in the b_n sequence is even and the rest are odd? Is there a way to state this question with a similar result modulo certain prime numbers? Create a new sequence from the terms $b_i + b_{i+1}$. Can we say anything about the parity of the terms in this sequence? Is there a way to classify which numbers appear "later"? For example, 7 appears in the sequence before 6 appears.

(b) Problem 2: Random Trees

We want to explore how we can randomly select a tree. One way to randomly select a tree is as follows. Pick a random permutation of $1, 2, \ldots, N$, where $N = \binom{n}{2}$, and assign this permutation of weight to the edges of the complete graph on $\{1, 2, \ldots, n\}$. Then find the minimum weight spanning tree for this graph. We notice that using this method will result in permutations that result in the same minimum spanning tree. The total number of trees we find using this method is $\binom{n}{2}!$.
Cayley's theorem says that the number of labeled trees on n vertices is n^{n-2}. The method above will vastly over count the number of labeled trees. We want to examine the trees that we find using this method. Do isomorphic trees appear

with the same probability? What about non-isomorphic trees? Does the Prüfer code or degree sequence tell us anything about the probability in which they appear?

II. **Computational algebra / algebraic geometry:**

(a) **Project 1.** Consider the polynomial ring, $k[x]$, in one variable over a field k. A set of polynomials $\{f, g\}$ is said to form a SAGBI bases if the leading monomials of f and g generate the algebra generated by the lead monomial of $k[f, g]$. The term SAGBI is an acronym for Subalgebra Analogue to Gröbner Bases for Ideals. Torstensson, *et.al.*, "Using resultants for SAGBI basis verification in the univariate polynomial ring" J. Symbolic Comput. **40** (2005), no. 3, $1087 - 1105$. They characterize when two such polynomials form a SAGBI bases. In this project we like to understand their work and address some generalizations
1.1. If f, g doesn't form a SAGBI bases, how many additional polynomials from $k[f, g]$ do we need so that the new set will form a SAGBI bases?
1.2. Can we get a similar result for three polynomials?

(b) **Project 2.** Consider the polynomial ring $k[x_1, \ldots, x_n]$ in n-variables. Let α be an element of the symmetric group S_n. α act on the variables x_i by $\alpha(x_i) = x_{\alpha(i)}$. Extend the action to any $f \in k[x_1, \ldots, x_n]$ by $\alpha(f(x_1, \ldots x_n)) = f(\alpha(x_1), \ldots, \alpha(x_n))$. An element $f \in k[x_1, \ldots x_n]$ is called invariant or fixed under action of α if $\alpha(f) = f$. The set of all invariant polynomials form a subalgebra of $k[x_1, \ldots, x_n]$. We will introduce the concept of SAGBI bases to study generators for such subalgebras. It is known that the ring of invariants of the alternating group A_n, $n \geq 3$ have no finite SAGBI bases with respect to any monomial ordering. But Manfred Göbel in "A finite SAGBI bases for polynomial invariants of conjugates of the Alternating Groups", Math. Comp. **71** (2002), no. 238, 761 - 765; showed that there is a non singular matrix $\delta_n \in GL_n(\mathbb{Z})$ such that the invariant ring of conjugate of the alternating group A_n w.r.t. δ_n have a finite SAGBI bases for lexicographic ordering. In this project;
2.1. One interesting problem of investigation is to understand δ_n more closely and identify other matrices with similar properties. (This problem is posed as open problem by Göbel him self)
2.2. Another problem is to study if similar result can be obtained for other monomial orders. (other than the Lexicographic order).

III. **Number Theory:**

(a) Amicable pairs for elliptic curves:

Recall that if we set $s(n)$ to be the function

$$s(n) = \sum_{\substack{d|n \\ d \neq n}} d,$$

then we say integers m, n form an amicable pair if $s(m) = n$ and $s(n) = m$. Silverman and Strange have generalized this to an elliptic curve $E/\mathbb{Q}$. In particular, if p, q are primes of good reduction for E they say they are an amicable pair if $\#E(\mathbb{F}_p) = q$ and $\#E(\mathbb{F}_q) = p$. Set

$$\mathcal{Q}_E(X) = \#\{\text{amicable pairs } (p, q) \text{ for } E/\mathbb{Q} \text{ with } p < q \text{ and } q \leq X\}.$$

In [**?**] it is conjectured (and a great deal of evidence supporting these conjectures is provided) that if E does not have complex multiplication then

$$\mathcal{Q}_E(X) \sim \frac{\sqrt{X}}{(\log X)^2}$$

and if E has complex multiplication there is a constant $A_E > 0$ so that

$$\mathcal{Q}_E(X) \sim A_E \frac{X}{(\log X)^2}$$

as $X \to \infty$.
Let K be a number field and let E/K be an elliptic curve. In this case, if $\mathfrak{p}$ and $\mathfrak{q}$ are primes of K, we say $(\mathfrak{p}, \mathfrak{q})$ is an amicable pair if $\#E(\mathbb{F}_\mathfrak{p}) = \mathrm{Nm}(\mathfrak{q})$ and $\#E(\mathbb{F}_\mathfrak{q}) = \mathrm{Nm}(\mathfrak{p})$. We will generalize the conjectures in [**?**] and investigate to what extent the results given there hold in the more general case. One would like to see to what extent the conjectures hold, how one can modify them if they do not hold, and if we can prove any of them on average.

(b) Lang-Trotter conjecture:

The distribution of primes has long been a central theme in number theory. One important conjecture in this area is the Lang-Trotter conjecture. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$ and let $a_E(p)$ denote the number of points on the reduction of E modulo the prime p. Let $r \in \mathbb{Z}$ and put $\pi_{E,r}(X) = \#\{p < X \mid p \text{ is prime and } a_E(p) = r\}$. Lang and Trotter [**?**] conjectured that if E does not have complex multiplication (this is true for almost all curves) or if $r \neq 0$, then

$$\pi_{E,r}(X) \sim C_{E,r} \frac{\sqrt{X}}{\log X}, \tag{1}$$

where the constant depends only on E and r. To appreciate the importance of this conjecture one should note that this is a refinement of the recently proved Sato-Tate conjecture and is more precise than what can be deduced from the Chebotarev density theorem in this setting.

(i) Champion primes:

An interesting related topic is the distribution of *champion primes* for an elliptic curve, that is a prime p for which $a_E(p)$ achieves the maximal/minimal value allowed by Hasse's theorem $\pm[|2\sqrt{p}|]$. Put

$$\begin{aligned}\pi_E^{\max}(X) &= \{p < X : a_E(p) = -\lfloor 2\sqrt{p}\rfloor\}\\ \pi_E^{\min}(X) &= \{p < X : a_E(p) = \lfloor 2\sqrt{p}\rfloor\}.\end{aligned}$$

Participants will compute the values of these functions for many curves E and for X as large as possible. They will combine these with heuristic arguments to formulate a conjecture on the asymptotic behavior of $\pi_E^{\max/\min}(X)$. They will also attempt to prove their conjecture holds on average as in the work of previous REUs [**?**, **?**].
Since the above problem may prove to be beyond elementary analytic techniques (even to obtain an average result), we will also consider related prime counting functions. Let $f(t)$ be a positive valued function which grows more slowly than $\sqrt{p}$ (-e.g. $f(t) = \log t$).

$$\pi_E^f(X) = \{p < X : a_E(p) = [|2\sqrt{p} - f(p)|]\}$$

(ii) Lang-Trotter Constant Computation:

The constant in the Lang-Trotter conjecture is given explicitly in terms of the Galois representations arising from E. However, it is difficult to explicitly compute the constant for a given curve E and integer r. In our 2003 REU, together with Bilbro and Manley, the Co-PIs investigated the Lang-Trotter conjecture computationally. In particular, we computed the ratio of primes $p < 10^7$ with $a_p(E) = r$ to $\sqrt{X}/\log X$ for various curves E, $r \in \mathbb{Z}$. In light of the Lang-Trotter conjecture, we expect that this ratio should tend to the constant $C_{E,r}$ of equation (1). In our 2008 REU, participants made some progress in developing algorithms to explicitly compute the constant $C_{E,r}$. Participants in future REUs will continue this work allowing one to extend the minimal computational evidence for the Lang-Trotter conjecture.

(iii) Lang-Trotter For Modular Forms:

The Lang-Trotter conjecture can be generalized to the setting of modular forms [**?**, **?**]. More generally, it can be formulated to the case of Galois representations for certain Galois representations. As a first step in this project we would produce more computational evidence for this form of the conjecture in the case of elliptic modular forms by using SAGE. Once the students are comfortable using SAGE, we would move on to studying the conjecture for Siegel modular forms. These are modular forms that live on Siegel upper half-space (a generalization of the complex upper half-plane) and transform under subgroups of $\mathrm{Sp}_{2n}(\mathbb{Z})$. In this setting there has been

no computational evidence, so we will produce the appropriate SAGE code to compute with such forms and then test the conjecture. In the case that $n = 2$ it is known these modular forms have an associated 4-dimensional Galois representation so we can also check whether these Galois representations fit into the class of representations the conjectures apply to.

(c) Extensions of Local Fields:

Given a prime p, one has the p-adic absolute value given by $\left|p^r \frac{a}{b}\right|_p = p^{-r}$ if $p \nmid ab$. One can complete $\mathbb{Q}$ with respect to this absolute value to obtain a local field $\mathbb{Q}_p$. In fact, it is known by a theorem of Ostrowski that along with the usual absolute value these are the only possible valuations on $\mathbb{Q}$. Furthermore, it is known that for a fixed degree n there are only finitely many extensions of $\mathbb{Q}_p$. John Jones and his collaborators have done a great deal of work into giving precise descriptions of the extensions for fixed degrees. There are two avenues of potential investigation here. First, one could consider a number field $K/\mathbb{Q}$ and complete K at a prime $\wp$. One could hope to determine the isomorphism classes of all field extensions of $K_\wp$ of a fixed degree.