POTENTIAL RESEARCH PROJECTS

GREG MARTIN
DRAFT: MAY 2, 2012

CONTENTS

1. PROBLEMS THAT STILL NEED TO BE PROCESSED

- add Ubis ch.3 "Questions of arithmetic and harmonic analysis"
- generalized difference-Sidon sets
- Granv/Sound/Wooley/Xu/Zhang (see desk)
- General local-to-global principle for Egyptian fractions with restricted denominators
- count pairs of subsets $A, B \subseteq \{0, \dots, n-1\}$ for which $|A+A| > |A+B|$? for which $|A-A| > |A+B|$?
- Let $f(n)$ equal the size of the smallest (primitive?) sum-dominant set contained in $\{1, \dots, n\}$ and containing 1 and n. How big is $f(n)$? (from Martin-O'Bryant: largest would be $n - O(1)$)
- sum-dominant subsets of $\{1, \dots, n\}$ of prescribed cardinality k. Do they still exist?
- absolutely simply abnormal numbers
- Selberg–Sathe (or earlier easier versions) for Beurling primes? Hawkins sieve?
- Shevelev phenomenon: there are always more primes with an odd number of 1s in their binary representation than there are with an even number of 1s
- Use Croot-type techniques on Egyptian fractions to greatly generalize Graham's general result on representations

2. Size of the largest Sidon set

A *Sidon set* is a set S where the pairwise sums $a + b$: $a, b \in S$ are all distinct (modulo $a + b = b + a$). For a survey of the subject of Sidon sets and a complete annotated bibliography of related work, see [O'B04].

Let $R(2, n)$ denote the size of the largest Sidon subset of $\{1, 2, \ldots, n\}$. It is known (see [MO06, p. 592] and [O'B04, Section 4.1]) that there exists a constant $0 < \delta < \frac{1}{2}$ such that

$$\sqrt{n} - n^{\delta} < R(2, n) < \sqrt{n} + n^{1/4} + 1,$$

where the lower bound holds for large enough n but the upper bound is universal. Erdős asked whether it is possible that $R(2, n)$ is always extremely close to $\sqrt{n}$; he offered \$500 to anyone who can settle this question (see [Guy04, C9]). (Although Erdős is no longer alive, these bounties are still being tracked and paid by Ron Graham on Erdős's behalf.)

Martin and O'Bryant [MO06, p. 603] propose an attack on this question. Most constructions of large Sidon sets proceed by constucting a Sidon set modulo some integer n (for example, the construction might take place in a finite field) and then noting that any Sidon set (mod n) remains a Sidon set when considered as a set of integers. Moreover, the (mod n) construction is usually preserved under affine transformations $x \mapsto ax + b$ (mod n). If one of these affine transformations ends up moving the whole Sidon set so that it does not intersect an interval $[m, n]$, then the resulting Sidon set is still large but is now a subset of $\{1, 2, \ldots, m\}$, resulting in a larger value for $R(2, m)$.

The goal, then, would be to analyze known constructions of (mod n) Sidon sets to see if a larger-than-average gap can be shown (or forced, using affine transformations) to exist. Several such constructions are summarized and described in [MO06].

Predicted level of problem: Hard to predict. Problem is very accessible to anyone with solid abstract algebra skills, but results in this area can be difficult to obtain. Analytic skills are probably necessary to investigate the distribution of gaps.

3. LINNIK-STYLE PROOF OF LEAST PRIME PRIMITIVE ROOT

For background on the relevant elementary number theory, see [NZM91]; for background on the relevant analytic number theory, see [MV07] or [IK04].

It is well known that every prime modulus q possesses primitive roots. We would still like to know more about how far we have to go before finding a primitive root (mod q), but we do at least know that there is a primitive root that is $\ll_\varepsilon q^{1/4+\varepsilon}$.

The question becomes more uncertain if we ask how far we have to go before finding a *prime* primitive root (mod q) (note that the smallest primitive root does not necessarily have to be prime, unlike the case for quadratic nonresidues say). At the moment, we cannot even show that all sufficiently large primes q possess a prime primitive root less than q itself! The best that can currently be done for this specific question is to take a specific residue class of primitive roots (mod q) and apply Linnik's theorem (specifically the current best version due to Xylouris [Xyl09]) to show that there exists a prime $p < q^{5.2}$ that is a primitive root for q.

In his dissertation Martin [Mar97, Mar98] investigated but did not successfully resolve this question; he showed that there exists a prime primitive root $p < q^\varepsilon$ if the generalized Riemann hypothesis is assumed, and $p < q^{3/4+\varepsilon}$ if there happens to be an exceptional zero (mod q), but no better bound than $q^{5.2}$ in general. However, Martin's approach was based purely on sieve methods; it might be that using the analytic techniques that go into Linnik's theorem would result in a much better bound.

The goal would be to understand the proof of Linnik's theorem well enough to adapt it to the case of multiple arithmetic progressions, specifically the set of primitive roots; hopefully the presence of multiple target arithmetic progressions would allow the exponent to be significantly decreased. Iwaniec and Kowalski [IK04] give an exposition of the original work of Linnik [Lin44a, Lin44b]. The most modern techniques are due essentially to Heath-Brown [HB92]; note that one might not have to look at his companion paper [HB90] where he dispenses with the case of an exceptional zero, since this has already been done in Martin's dissertation. It's hard to know in advance whether the multiple residue classes make the problem much easier (so that only the original idea of Linnik is necessary), possible but difficult (so that numerical optimizations of the sort Heath-Brown introduced are necessary), or simply do not help at all.

Predicted level of problem: PhD project.

4. SPECIAL THREE-WAY PRIME NUMBER RACES

See Granville and Martin [GM06] for a survey of prime number races.

A *three-way prime number race* concerns a modulus q, three distinct reduced residue classes $a, b, c \pmod q$, and the inequalities

$$\pi(x; q, a) > \pi(x; q, b) > \pi(x; q, c), \tag{1}$$

where $\pi(x; q, a)$ counts the number of primes up to x that are congruent to $a \pmod q$. Rubinstein and Sarnak [RS94] proved (under certain strong hypotheses on the zeros of Dirichlet L-functions) that the inequalities (1) hold for a positive proportion of positive real numbers x. Using their methods, Feuerverger and Martin [FM00] wrote down a formula for calculating the exact density $\delta(q; a, b, c)$ of positive real numbers x for which the inequalities (1) hold.

Later, Fiorilli and Martin [FM09] investigated two-way prime number races in more detail, focusing in part on the question of determining which densities $\delta(q; a, b)$ are larger and smaller as a, b vary and q remains fixed. The same question was addressed by Lamzouri [Lam11] for prime number races among three or more residue classes.

However, there are certain three-way prime number races for which one should be able to obtain more explicit results than Lamzouri's. When a, b, c have the property that $a^2 \equiv b^2 \equiv c^2 \pmod q$ (as is the case in the two examples considered in [Mar02]), there is an approach to analyzing the size of the densities $\delta(q; a, b, c)$ that is more similar to the simpler Fiorilli–Martin approach than to the more involved Lamzouri approach.

The goal would be to analyze these particular three-way prime number races using the techniques of Fiorilli–Martin, deriving an asymptotic formula for $\delta(q; a, b, c)$ that is precise enough to compare the densities to one another.

Predicted level of problem: MSc thesis or early PhD project.

5. Beurling–Nyman criterion for the Riemann hypothesis and connections to sieves

See physical folder on desk.

6. RANDOM SIEVES

Describe Hawkins random sieve.

Instead of selecting $1/X_n$ integers at random to remove, what happens if your select one of the arithmetic progressions (mod X_n) at random to remove? Do we end up with realistic distribution in arithmetic progressions? in short intervals (a la Mayer)? Arithmetic factors in Mertens' formula?

Lorch/Ökten [LÖ07] is a good survey article about the Hawkins random sieve, including references to other such papers. Bui and Keating [BK06] is one recent paper that looks well-written.

Grimmett and Hall [GH91] have a "stationary" random sieve that removes arithmetic progressions, but does not have the aspect of letting the next arithmetic progression's modulus equal the smallest unprocessed number currently still in the set, as the Hawkins random sieve does.

REFERENCES

[BK06] H. M. Bui and J. P. Keating. On twin primes associated with the Hawkins random sieve. *J. Number Theory*, 119(2):284–296, 2006.

[FM00] Andrey Feuerverger and Greg Martin. Biases in the Shanks-Rényi prime number race. *Experiment. Math.*, 9(4):535–570, 2000.

[FM09] Daniel Fiorilli and Greg Martin. Inequities in the shanks-renyi prime number race: An asymptotic formula for the densities. *arXiv*, (0912.4908), 12 2009.

[GH91] G. R. Grimmett and R. R. Hall. The asymptotics of random sieves. *Mathematika*, 38(2):285–302 (1992), 1991.

[GM06] Andrew Granville and Greg Martin. Prime number races. *Amer. Math. Monthly*, 113(1):1–33, 2006.

[Guy04] Richard K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, third edition, 2004.

[HB90] D. R. Heath-Brown. Siegel zeros and the least prime in an arithmetic progression. *Quart. J. Math. Oxford Ser. (2)*, 41(164):405–418, 1990.

[HB92] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc. (3)*, 64(2):265–338, 1992.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Lam11] Youness Lamzouri. Prime number races with three or more competitors. *arXiv*, (1101.0836), 01 2011.

[Lin44a] U. V. Linnik. On the least prime in an arithmetic progression. I. The basic theorem. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):139–178, 1944.

[Lin44b] U. V. Linnik. On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):347–368, 1944.

[LÖ07] John Lorch and Giray Ökten. Primes and probability: the Hawkins random sieve. *Math. Mag.*, 80(2):112–119, 2007.

[Mar97] Greg Martin. The least prime primitive root and the shifted sieve. *Acta Arith.*, 80(3):277–288, 1997.

[Mar98] Greg Martin. Uniform bounds for the least almost-prime primitive root. *Mathematika*, 45(1):191–207, 1998.

[Mar02] Greg Martin. Asymmetries in the Shanks-Rényi prime number race. In *Number theory for the millennium, II (Urbana, IL, 2000)*, pages 403–415. A K Peters, Natick, MA, 2002.

[MO06] Greg Martin and Kevin O'Bryant. Constructions of generalized Sidon sets. *J. Combin. Theory Ser. A*, 113(4):591–607, 2006.

[MV07] Hugh L. Montgomery and Robert C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons Inc., New York, fifth edition, 1991.

[O'B04] Kevin O'Bryant. A complete annotated bibliography of work related to Sidon sequences. *Electron. J. Combin.*, DS11 (Dynamic Survey), 2004.

[RS94] Michael Rubinstein and Peter Sarnak. Chebyshev's bias. *Experiment. Math.*, 3(3):173–197, 1994.

[Xyl09] Triantafyllos Xylouris. On linnik's constant. *arXiv*, (0906.2749), 06 2009.