# Some problems related to Singer sets

Alex Chmelnitzki

October 24, 2005

## Preface

The following article describes some of the work I did in the summer 2005 for Prof. Ben Green, Bristol University. The work was very computational in flavour, partly because computations were the natural first course of attack for most of the problems Ben Green posed me and partly because two months turned out to be not enough to complement the computational results by substantial theoretical work. However, the pictures and numbers I obtained suggested certain conjectures, which I hope to be able to prove or disprove in the future.

I used the programming language C++ and the Microsoft Visual C++ compiler for all computationally "expensive" tasks and Maple in most cases where I needed nice pictures at the end. In some cases I combined the two by first outputting the numbers into a file and then importing the file in Maple to produce diagrams. I have not included the source code for the programs here but I will be very happy to supply it on demand.

## Contents

**1 Sidon, Singer and finite sets 2**

**2 Some properties of Singer sets and some definitions 3**

**3 The discrete Fourier transform 4**

**4 Litllewood's conjecture and Singer sets 6**

**5 Conclusion 9**

# 1 Sidon, Singer and finite sets

In 1932 Simon Sidon asked Paul Erdős how large a subset S of $\{0, 1, \ldots, N\}$ can be if it has the property that every natural number arises in at most one way as the difference of two elements of S, in other words if $\forall\ a, b, c, d \in S, a-b = c-d \Rightarrow$ either $a = c$, $b = d$ or $a = b$, $c = d$. This condition is equivalent to saying that the representation of a natural number as a sum of two elements of S is essentially unique if it exists, by which we mean that $\forall\ a, b, c, d \in S, a+b = c+d \Rightarrow$ either $a = c$, $b = d$ or $a = d$, $b = c$. Sets with this property are now referred to as Sidon sets.

Erdős answered Sidon's question as follows (see [3], a more general approach can be found in [6]): if s(N) denotes the size of the largest Sidon subset of $\{0, 1, \ldots, N\}$ then $s(N) = O(N^{1/2})$. Subsequently other mathematicians showed that this bound is tight by finding algorithms which generate Sidon sets with size about $\sqrt{N}$. All known constructions proceed by first finding a Sidon set modulo a prime and then "'unwrapping"' it. That is to say if $S \subseteq \mathbb{Z}/q\mathbb{Z}$ is a Sidon set (this time the differences are considered modulo q) then define $A \subseteq \{1, 2, \ldots, N\}$ by saying $x \in A$ if and only if $x$(mod q)$\in S$. One of these algorithms is due to James Singer (for details see [7]). Singer was not actually working on number theory but on finite projective geometry when he found this algorithm. It was only after he had proven a theorem in geometry that he realised the number theoretic application. This is Singer's theorem in number theoretic terms: Let p be a prime and let $q = p^2 + p + 1$. Then $\exists\ A \subseteq \mathbb{Z}/q\mathbb{Z}$ with $|A| = p + 1$ such that $\forall\ x \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\}\ \exists\ a_1, a_2 \in A$ such that $x = a_1 - a_2$. Such a set, in which every non-zero difference (modulo q) arises not only at most once but exactly once is called a perfect difference set.

The construction Singer invented uses properties of finite fields. It works as follows: Let p be a prime and let $\mu$ be a primitive element in $\mathbb{F}_{p^3}$. Then $\left\{1, \mu, \mu^2\right\}$ is a basis for $\mathbb{F}_{p^3}$ over $\mathbb{F}_p$. Hence every element of $\mathbb{F}_{p^3}$ is uniquely expressible as a linear combination of $1, \mu$ and $\mu^2$ with coefficients in $\mathbb{F}_p$. Now, take all elements for which the coefficient of $\mu^2$ is 0 and the coefficient of $\mu$ is 1 and reduce these elements modulo q. The resulting set together with 0 has p+1 elements and is a perfect difference set.

Now, how would we, or for that matter the computer, go about generating such sets? First of all we need to find a primitive element $\mu$ of $\mathbb{F}_{p^3}$ and we need to be able to express all elements of $\mathbb{F}_{p^3}$ as a linear combination of $1, \mu$ and $\mu^2$ with coefficients in $\mathbb{F}_p$. There are many ways of doing this, some more efficient than others. We recall that if the element $\mu$ is primitive, $\mu^n \neq 1 \forall\ n < p^3 - 1$. Thus the field $\mathbb{F}_{p^3}$ consists of the elements $\left\{0, \mu, \mu^2, \ldots, \mu^{p^3-1}\right\}$. So here is a naive approach to generating Singer sets:

- We start by finding an irreducible polynomial in $\mathbb{F}_p$ of degree 3. Again, there are many ways of checking whether or not such a polynomial is irreducible. The easiest (although one of the slowest) is to substitute in all values between 0 and p-1 and to check if any one of them is a root in $\mathbb{F}_p$. Another method is to use Euclid's algorithm to find the highest common factor between the polynomial in question and $x^p - x$. This works because every element of $\mathbb{F}_p$ is a root of the latter. Finally, there is a method which works particularly well for polynomials of degree 2 and 3: Use Cardano's formula for the roots of the cubic polynomial. The polynomial is reducible if and only if all the quadratic roots involved exist. This comes down to checking if given elements are quadratic residues modulo p and finding some quadratic roots. Again, there are quite fast methods to do this, which can not be covered here. For detailed descriptions of these and other algorithms see [2].

- Once we have found an irreducible polynomial of degree 3 we have to hope that its roots are primitive and if they are not then we need to try the next irreducible polynomial. How do we find that out? Let $\mu$ be a root of the polynomial. First, we can use the polynomial itself to express $\mu^3$ in terms of its lower powers. Now we use $\mu^4 = \mu^3 \times \mu$ and substitute in our expression for $\mu^3$ twice until we get another expression which involves only the 0th, 1st and 2nd powers of $\mu$. We can keep going like this until we have expressed all the powers of $\mu$ up to $\mu^{p^3-1}$ in terms of $1, \mu$ and $\mu^2$. If any one of these expressions apart from the last one turns out to be 1 then $\mu$ is not primitive. If it is primitive, then we can use our calculation in the next step to compute a Singer set. However, we don't actually need to check all the powers to find out whether $\mu$ is primitive. Since we know that $\mu^{p^3-1} = 1$ it suffices to check only those powers that divide $p^3 - 1$. In particular, once we know that $\mu^n \neq 1 \; \forall \; n \leq (p^3 - 1)/2$, we know that $\mu$ is primitive.

- We now have a generator $\mu$ for $\mathbb{F}_{p^3}$ over $\mathbb{F}_p$ and we have expressions for all the elements of $\mathbb{F}_{p^3}$ in terms of the basis $\left\{1, \mu, \mu^2\right\}$. We are nearly done. If we write $\mu^n = a_n + b_n\mu + c_n\mu^2$ where $n \in \left\{0, 1, \ldots, p^3 - 2\right\}$ and $a_n, b_n, c_n \in \mathbb{F}_p$, then the set $\{0\} \cup \{n : b_n = 1, c_n = 0\}$ reduced modulo $p^2 + p + 1$ is the required Singer set!

## 2 Some properties of Singer sets and some definitions

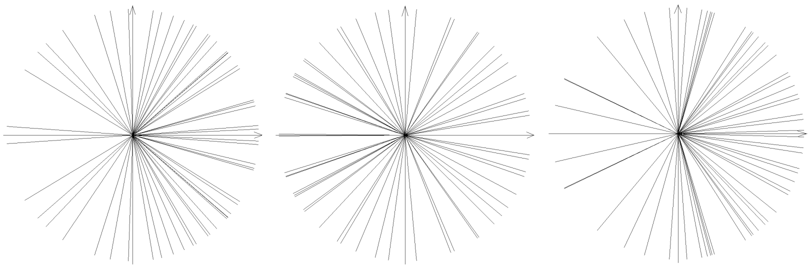
First of all a Singer set is a perfect difference set and thus a Sidon set. It has p+1 elements for some prime p and every number between 1 and $p^2 + p$ occurs exactly once as a difference of two elements of such a set modulo $p^2 + p + 1$. Further, if S is a Singer set, a is any natural number and b is a natural number coprime to $p^2+p+1$, then $aS+b = \{ax + b : x \in S\}$ is also a Singer set. However, it is possible that for certain $(a, b) \neq (1, 0)$ aS+b = S. We will introduce some useful notions:

**Definition 2.1.** *Let $S \subseteq \mathbb{Z}/q\mathbb{Z}$ be a Singer set, let $(a, q) = 1$. We say that the Singer set aS is S* ***dilated*** *by a, the Singer set S+b is S* ***translated*** *by b.*

**Definition 2.2.** *The Singer set S is* ***normal*** *if $0 \in S, 1 \in S$.*

**Remark 2.3.** *Note that since for any Singer set $S \; \exists \; x, y \in S$ such that $x - y = 1$[1], we can always* ***normalise*** *a Singer set by translating it by $-y$.*

[1] we are still working modulo q here



(a) Original Singer set (b) translated by 1 (c) translated by 2

Figure 1: The effect of translating a Singer set on its Fourier transform

But the actual focus of this work shall be put onto some more hidden properties of Singer sets. More information about Singer sets and related publications can be found in [5].

# 3 The discrete Fourier transform

**Definition 3.1.** *Let $S \subseteq \mathbb{Z}/q\mathbb{Z}$ be a Singer set. We define the* ***discrete Fourier Transform*** *of $S$ by*

$$\widehat{S}(r) = \sum_{x \in S} e^{2\pi i r x/q}$$

*for each $r \in \mathbb{Z}/q\mathbb{Z}$.*

Let us make some observations. First of all $\widehat{S}(0) = |S|$. However, more interestingly we have the following

**Lemma 3.2.**

$$|\widehat{S}(r)| = \sqrt{p} \; \forall \; r \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\} .$$

*Proof.* For each $r \neq 0$

$$|\widehat{S}(r)|^2 = \widehat{S}(r)\overline{\widehat{S}(r)} = \sum_{x,y \in S} e^{2\pi i (x-y)/q}.$$

However as $x$,$y$ range over S, $x - y$ takes each non-zero value modulo q exactly once and it takes the value 0 exactly p times, so we get

$$|\widehat{S}(r)|^2 = p + \sum_{t=0}^{q-1} e^{2\pi i r t/q} = p.$$

Hence the result! □

Now, what about $\arg(\widehat{S}(r))$? One question would be how uniform is it distributed in $[0, 2\pi)$ as r varies? The first thing to note is that if $R = aS$ where a is co-prime to q then $\arg(\widehat{R}(r)) = \arg(\widehat{S}(ar))$. Since $(a, q) = 1$, $ar$ takes all values modulo q as r varies, so dilating the set by $a$ does not change the distribution of the arguments in $[0, 2\pi)$ as r varies. On the other hand, if $T = S + b$ then $\arg(\widehat{T}(r)) = \arg(\widehat{S}(r)) + 2\pi rb/q$. This does change the distribution of the arguments. To illustrate this, consider the Figure 1. Here $p = 7$, the original Singer set is 0, 1, 6, 15, 22, 26, 45, 55 and each pictures shows the values for $\widehat{S}(r)$ for all values of r in 0,1,...,q-1, each with a different translation of the original Singer set.

Obviously, we cannot answer any questions about the distribution of the argument for different r just by looking at pictures. We want to be able to quantify the extent of uniformity of a distribution, so we make the following

**Definition 3.3.** *Given a finite set $P \subset [a, b]$ and $\alpha \in [a, b), \beta \in (a, b]$ with $\alpha < \beta$, write $D(\alpha, \beta) = |P| \times (\beta - \alpha)/(b - a) - |P \cap (\alpha, \beta)|$. Then we can define the* ***discrepancy*** *of $P$ by $\mathfrak{D}^*(P) = \frac{1}{|P|} \times \overset{sup}{\alpha,\beta}\ D(\alpha, \beta)$.*

In particular if the values in P are perfectly uniformly distributed over [a,b], then $\mathfrak{D}^*(P) = 1/|P|$. If on the other hand $x = a\ \forall\ x \in P$ then $\mathfrak{D}^*(P) = 1$. In our case we need to also take care of the fact that 0 is identified with $2\pi$.

The first natural course of attack in our case is to try to compute the discrepancies of the arguments of the Fourier transforms for different Singer sets and see if we can notice any regularities as p gets large. Unfortunately, the discrepancy is a computationally expensive quantity. The algorithm I used to compute it works as follows:

- Compute the Singer set in question.
- Then compute the arguments of the Fourier transform of this Singer set for all values of r.
- Sort the arguments in an array.
- Append the same array but each value increased by $2\pi$.
- Look for the biggest interval $(\alpha_0, \beta_0)$ containing no values and compute $D(\alpha_0, \beta_0)$. Then do the same for intervals containing exactly one value and see if $D(\alpha_0, \beta_0) > D(\alpha_1, \beta_1)$. By continuing like this find n such that for the biggest interval $(\alpha_n, \beta_n)$ containing exactly n values, $D(\alpha_n, \beta_n)$ is maximal among all n.
- Now, $\mathfrak{D}^* = \frac{1}{|S|} D(\alpha_n, \beta_n)$.

I ran this computation for various p. I confined myself to p for which $p^2 + p + 1$ is prime, so that once the computer found a Singer set, it could experiment with translating and dilating it without worrying about the dilation factor being coprime to q. Unfortunately it is an open question, whether there are infinitely many such p, but for experimental purposes there are enough small ones. These are some of the numbers I got:

| p | highest discr. | lowest discr. |
|---|---|---|
| 5 | 0.349 | 0.180 |
| 101 | 0.135 | 0.018 |
| 167 | 0.057 | 0.009 |
| 173 | 0.127 | 0.004 |

This led me to make the following

**Conjecture 3.4.** *Given $\epsilon > 0$ $\exists$ a prime $p_0$ such that $\forall p > p_0$ there is a Singer set modulo $p^2 + p + 1$ with its discrepancy being smaller than $\epsilon$.*

Being a bit braver one could go further:

**Conjecture 3.5.** *Given $\epsilon > 0$ $\exists$ a prime $p_0$ such that $\forall p > p_0$, the discrepancy of all Singer sets modulo $p^2 + p + 1$ is less than $\epsilon$.*

However, in my opinion the numbers are not quite enough of a justification for that. Some information about discrepancies for much larger p would help here.

# 4 Litllewood's conjecture and Singer sets

Obviously, Littlewood made quite a few conjectures and in particular some of them are called Littlewood's conjecture [1]. The one we are interested in is the following:

**Conjecture 4.1.** *(Flat polynomials on the unit circle) There exist constants $0 < c_1 < c_2$, an infinite sequence of integers $n$, and polynomials $p_n$ of the form $\epsilon_0 + \epsilon_1 z + \ldots + \epsilon_{n-1} z^{n-1}$, where $\epsilon_j \in \{-1, 1\}$, such that*

$$c_1\sqrt{n} \leq |p_n(z)| \leq c_2\sqrt{n}$$

*for all $z \in \mathbb{C}$ with $|z| = 1$.*

No polynomials are known which satisfy just the lower bound, however just the upper bound can be satisfied with the so called Rudin-Shapiro polynomials.

A rather natural approach to this problem is to try sequences of signs which fluctuate quite randomly. One example that has been tried (the Fekete polynomials) is to take $n = q$ and $\epsilon_j = (j|q)$, the Legendre symbol. Unfortunately this does not work. For details see [4]. Ben Green had the following idea:

Let $q = p^2 + p + 1$ and let $A \subseteq \mathbb{Z}/q\mathbb{Z}$ be a Singer set. Let $B = A + A = a + a' : a, a' \in A$. From the properties of Singer sets we know that if $x = a + a'$ then this representation is essentially unique: there is one representation if $a = a'$ and there are two if $a \neq a'$, namely $x = a + a' = a' + a$. Hence we can compute that $|B| = \frac{1}{2}(p^2 + 3p + 2)$, so B consists of about half the residues (mod $q$). We have the following result:

**Lemma 4.2.** *Let $f_q(z) = \epsilon_0 + \epsilon_1 z + \ldots + \epsilon_{q-1} z^{q-1}$ be the polynomial defined by $\epsilon_j = 1$ if $j \in B$, and $\epsilon_j = -1$ otherwise. Then*

$$f_q(e^{2\pi i r/q}) = \widehat{A}(r)^2 + \widehat{A}(2r)$$

*for $r = 1, \ldots, q-1$ and*

$$f_q(1) = 2p + 1.$$

*In particular, in view of 3.2 these polynomials satisfy both the upper and the lower bound of Littlewood's conjecture when z is a q-th root of unity.*

*Proof.*

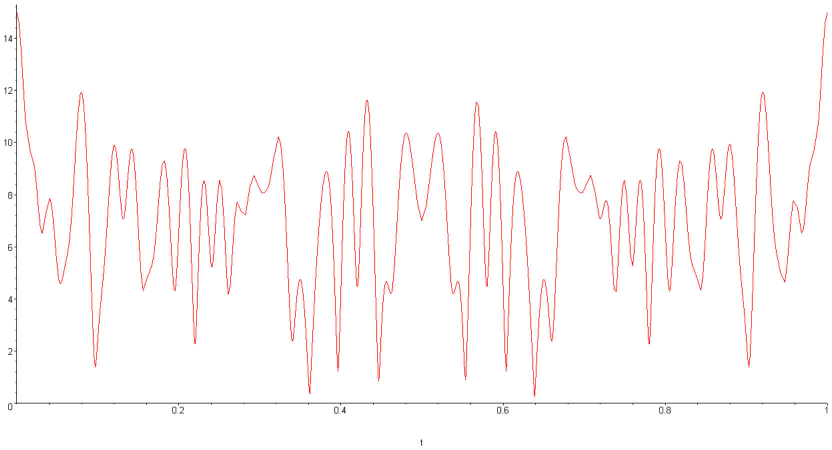
$$\begin{aligned}
f_q(e^{2\pi ir/q}) &= \sum_{j\in A+A} e^{2\pi irj/q} - \sum_{j\notin A+A} e^{2\pi irj/q} \\
&= \sum_{j\in A+A} e^{2\pi irj/q} + \sum_{j\in A+A} e^{2\pi irj/q} - \sum_{j\in A+A} e^{2\pi irj/q} - \sum_{j\notin A+A} e^{2\pi irj/q} \\
&= 2\sum_{j\in A+A} e^{2\pi irj/q} - \underbrace{\sum_{j=0}^{q-1} e^{2\pi irj/q}}_{=0} \\
&= \underbrace{2\sum_{\substack{j=a+a',\\ a\neq a'}} e^{2\pi irj/q} + \sum_{\substack{j=2a\\ a\in A}} e^{2\pi irj/q}}_{\widehat{A}(r)^2} + \underbrace{\sum_{\substack{j=2a\\ a\in A}} e^{2\pi irj/q}}_{\widehat{A}(2r)}
\end{aligned}$$

Also

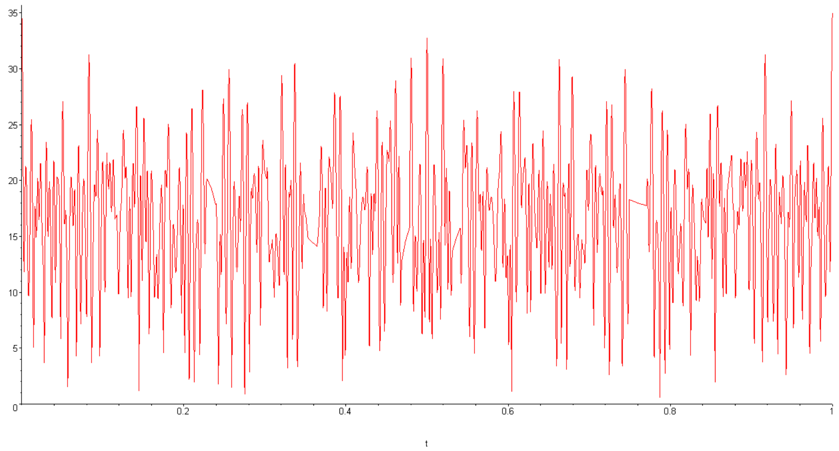
$$\begin{aligned}
f_q(1) &= \sum_{j\in A+A} 1 - \sum_{j\notin A+A} 1 \\
&= \frac{1}{2}(p^2+3p+2) - \frac{1}{2}(p^2-p) \\
&= 2p+1
\end{aligned}$$

□

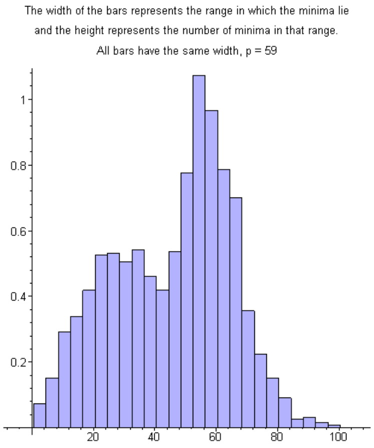
This observation led Ben Green to suggest that these polynomials could solve Littlewood's conjecture. So the main question was, how $|f_q|$ behaves between the q-th roots of unity. Again, we decided to first look at the problem computationally. Here is for example the plot of the absolute value of this polynomial on the unit circle for $p = 7$:

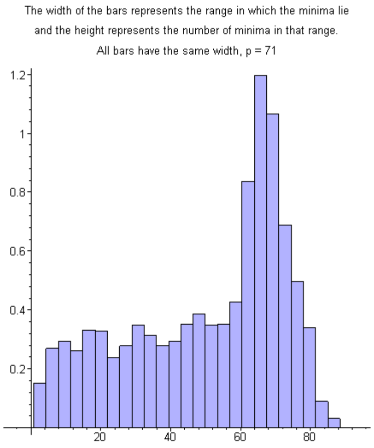


Here is the plot for $p = 17$:



It is obvious that it does not make much sense to plot polynomials for higher p since they fluctuate too much. However, it turns out that while the maximum does not seem to go far beyond $2p+1$ which is the value of the polynomial at 1, the minimum seems to be very low even for large p. This may seem quite surprising because the absolute value of the polynomials is within a rather narrow corridor on points that get denser and denser as p gets bigger. But between these points it "manages" to get nearly to 0. So, to understand the behaviour of these polynomials a bit better, we decided to look at the distribution of the minima between q-th roots of unity, i.e. for each $r \in \{0, ..., q-1\}$ I computed $\overset{min}{\theta\in[r,r+1)} f\left(e^{\frac{2\pi i\theta}{q}}\right)$. Here are two histograms for $p = 59$ and $p = 71$, respectively:


The width of the bars represents the range in which the minima lie and the height represents the number of minima in that range. All bars have the same width, p = 59


The width of the bars represents the range in which the minima lie and the height represents the number of minima in that range. All bars have the same width, p = 71

It is very clear that the distribution of the minima must be tending to some distribution as p tends to infinity. My guess would be that it is the turned over log-normal, but this would have to be proven. What we can say with certainty by looking at the pictures (also at those for bigger p which I did not plot here) is that there are always some points that are only just above zero. Hence

**Conjecture 4.3.** *Let $f_q$ be as above. Then $\overset{sup}{|z|=1} |f_q(z)| = O(q^{1/2})$ but there is no constant $c$ such that $c\sqrt{q} \leq |f_q(z)|$ for all $q = p^2 + p + 1$ and for all $z \in \mathbb{C}$ with $|z| = 1$.*

To prove the latter, there might be several possibilities, none of which I have fully explored:

- One can try to look at the midpoints between the q-th roots of unity and show that the minimum of $|f_q(z)|$ among these midpoints is smaller than something of order $\sqrt{q}$. This technique already worked to show that the Fekete polynomials do not satisfy the lower bound.
- One can look at those points at which $\frac{d}{dt}\left(f_q(e^{ti})\overline{f_q(e^{ti})}\right) = 0$ and show that the minimum of $|f_q(z)|$ among these points is smaller than something of order $\sqrt{q}$.

The second technique might also work to show that the maximum of $|f_q(z)|$ on the unit circle is of order $\sqrt{q}$. All this belongs to my future projects.

# 5 Conclusion

There are many other questions that one can ask about Singer sets. Some questions that I posed and that do not seem to have been answered are the following:

**Definition 5.1.** *I will call two Singer sets* ***essentially different*** *if their normalized versions are different, i.e. if one cannot be translated into the other.*

**Problem 5.2.** *How many essentially different Singer sets of a given order are there?*

This question would be answered by an answer to the following:

**Problem 5.3.** *Given a Singer set $S \subseteq \mathbb{Z}/q\mathbb{Z}$ and an integer $a$ co-prime to $q$, when are $S$ and $aS$ essentially different?*

To illustrate the latter, consider the Singer set $S =$ 0,1,3,9 modulo 13. Then $3S = S$!
Finally, the third question that I found very natural to ask after having worked with Singer sets was

**Problem 5.4.** *Sometimes, generators for $\mathbb{F}_{p^3}$ over $\mathbb{F}_p$ that arise from different irreducible polynomials produce the same Singer set. What is the relation between such irreducible polynomials?*

I think that a good answer to any one of these questions should answer the other two, as well. All in all, this work certainly taught me much better what we don't know rather than what we know, but it opened up lots of perspectives for further investigations.

# References

[1] Peter Borwein. *Computational excursions in analysis and number theory.* CMS Books in Mathematics; 10. Springer, New York, 2002.

[2] Henri Cohen. *A course in computational number theory.* Graduate texts in mathematics; 138. Springer, Berlin, 1993.

[3] P. Erdős and P. Turán. On a problem of sidon in additive number theory, and on some related problems. *J. London Math. Soc.*, 16:212–215, 1941.

[4] Hugh L. Montgomery. An exponential polynomial formed with the legendre symbol. *Acta Arith.*, 37:375–380, 1980.

[5] Kevin O'Bryant. A complete annotated bibliography of work related to sidon sequences.

[6] Imre Z. Ruzsa. Solving a linear equation in a set of integers i. *Acta Arith.*, 65(3):259–282, 1993.

[7] James Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43:377–385, 1938.