Searching for Defective Prime Powers (in Low Genus)

Katie Ahrens[1] Jon Grantham[2]

[1]Institute for Defense Analyses
Center for Communications Research
La Jolla, CA
[2]Institute for Defense Analyses
Center for Computing Sciences
Bowie, MD

May 2025

Center for Computing Sciences
17100 Science Drive • Bowie, Maryland 20715

Introduction

- Serre's "Rational Points on Curves over Finite Fields" is the jumping-off point for determining how many points a curve over a finite field can have.
- We have from the Hasse-Weil bound that the largest number of points for a genus g curve over $\mathbb{F}_q$ is $q + 1 + g\lfloor 2\sqrt{q} \rfloor$.
- When this bound is not achieved, we say that q has a "defect" based on the extent to which the bound is missed.
- E.g., if the maximum is $q + g\lfloor 2\sqrt{q} \rfloor$, we say that q has "defect 1" (in genus g).
- Serre gives conditions on prime powers q that determine when there is a defect.

Introduction

- Serre's "Rational Points on Curves over Finite Fields" is the jumping-off point for determining how many points a curve over a finite field can have.
- We have from the Hasse-Weil bound that the largest number of points for a genus g curve over $\mathbb{F}_q$ is $q + 1 + g\lfloor 2\sqrt{q} \rfloor$.
- When this bound is not achieved, we say that q has a "defect" based on the extent to which the bound is missed.
- E.g., if the maximum is $q + g\lfloor 2\sqrt{q} \rfloor$, we say that q has "defect 1" (in genus g).
- Serre gives conditions on prime powers q that determine when there is a defect.
- As a result, this is a computational number theory talk, not an arithmetic geometry talk.

Introduction

- Serre's "Rational Points on Curves over Finite Fields" is the jumping-off point for determining how many points a curve over a finite field can have.
- We have from the Hasse-Weil bound that the largest number of points for a genus g curve over $\mathbb{F}_q$ is $q + 1 + g\lfloor 2\sqrt{q} \rfloor$.
- When this bound is not achieved, we say that q has a "defect" based on the extent to which the bound is missed.
- E.g., if the maximum is $q + g\lfloor 2\sqrt{q} \rfloor$, we say that q has "defect 1" (in genus g).
- Serre gives conditions on prime powers q that determine when there is a defect.
- As a result, this is a computational number theory talk, not an arithmetic geometry talk.
- I have disappointed half of you and excited the other half.

Genus 1

- Genus 1 is the elliptic curve case.
- Let $m = \lfloor 2\sqrt{q} \rfloor$.
- Theorem: There is a defect if and only if $q = p^e$, e odd, $p > 3$, and $p|m$.
- Consequence of work of Deuring (1941) and Waterhouse (1969).

Genus 1, $e = 1$

- $m = \lfloor 2\sqrt{p} \rfloor$.
- Can you have $p|m$?
- Requires $2\sqrt{p} > p$, so $4 > p$.

Genus 1, $e = 3$

- $m = \lfloor 2\sqrt{p^3} \rfloor$.
- Can you have $p|m$?
- That would give us $4p^3 = m^2 + \epsilon$ with $1 \leq \epsilon \leq 2m < 4p^{3/2}$.
- If $m = p\mu$, then $4p^3 = p^2\mu^2 + \epsilon$.
- Hence $p^2|\epsilon$ and $p^2 < 4p^{3/2}$.
- This means $p < 16$, and we check that $p \not| m$ for these cases.)
- (Serre, pp. 23–24, but there's a typo: he says $p|m$ when $p < 16$.)

Genus 1, $e = 5$

- We don't know of any obstruction when $e \geq 5$ (neither does Serre).
- He searched up to 10^9, and 7 was the only example.
- He notes that "a naive log log argument suggest that there should be some very sparse larger ones."
- We would like to call these *Serre primes*.

Genus 1, $e = 5$

- We don't know of any obstruction when $e \geq 5$ (neither does Serre).
- He searched up to 10^9, and 7 was the only example.
- He notes that "a naive log log argument suggest that there should be some very sparse larger ones."
- We would like to call these *Serre primes*.
- We searched up to 10^{16} and didn't find any.

The naive log log argument

- Without any known obstruction, we assume that $m = \lfloor 2\sqrt{p^5} \rfloor$ is chosen at random mod p.
- In particular, the chance that $p|m$ is $1/p$.
- So the expected number of p with $y < p < x$ and $p|m$ is $\sum_{y<p<x} 1/p \approx \log\log(x) - \log\log(y)$.
- $\log\log(10^{16}) - \log\log(10^9) \approx 0.57$, so we weren't incredibly unlucky.

The naive log log argument, $e \geq 7$

- Given how rare these primes are likely to be, how do we test the heuristic?
- (After all, maybe we are unaware of an obstruction.)
- The log log argument should apply for all odd $e \geq 5$.
- So let's look at $7 \leq e < 107$.
- $\log\log(10^{11}) - \log\log(10^2) \approx 1.7$, so we should find about 85 es across that range.
- (I'm not sure if it makes sense to exclude the low end, but we did just to be safe.)

The naive log log argument, $e \geq 7$

- Given how rare these primes are likely to be, how do we test the heuristic?
- (After all, maybe we are unaware of an obstruction.)
- The log log argument should apply for all odd $e \geq 5$.
- So let's look at $7 \leq e < 107$.
- $\log\log(10^{11}) - \log\log(10^2) \approx 1.7$, so we should find about 85 es across that range.
- (I'm not sure if it makes sense to exclude the low end, but we did just to be safe.)
- There are 84.

Deuring-Waterhouse Numbers

- Sequence A364690 of the Online Encyclopedia of Integer Sequences consists of the prime powers with defects.
- It was computed up to 10^{18}.
- We extended that to 10^{70}.
- We would like to call them *Deuring-Waterhouse numbers*.

Deuring-Waterhouse Numbers up to 10^{70}

2^{7}, 2^{11}, 3^{7}, 7^{5}, 2^{15}, 2^{17}, 2^{19}, 5^{9}, 2^{21}, 2^{23}, 3^{15}, 5^{11}, 2^{27}, 2^{29}, 5^{15}, 2^{39}, 3^{25}, 2^{41}, 5^{19}, 2^{47}, 2^{49}, 2^{55}, 2^{57}, 3^{37}, 113^{9}, 5^{27}, 13^{17}, 3^{41}, 3^{43}, 13^{19}, 239^{9}, 2^{73}, 3^{47}, 2^{75}, 7^{29}, 2^{83}, 3^{53}, 5^{37}, 5^{39}, 2^{93}, 2^{95}, 37^{19}, 2^{101}, 2^{103}, 3^{65}, 2^{107}, 13^{29}, 2^{109}, 3^{69}, 2^{113}, 2^{115}, 2^{117}, 5^{51}, 3^{75}, 2^{119}, 2^{123}, 2^{125}, 2^{127}, 2^{131}, 3^{85}, 747343^{7}, 2^{137}, 7^{49}, 3^{87}, 43783^{9}, 2^{139}, 2^{143}, 3^{91}, 13^{39}, 79^{23}, 3^{97}, 2^{155}, 23^{35}, 5^{69}, 2^{161}, 2^{163}, 3^{103}, 2^{165}, 3^{105}, 13^{45}, 17^{41}, 2^{169}, 3^{107}, 2^{171}, 3^{109}, 2^{177}, 73877^{11}, 109^{27}, 2^{183}, 2^{185}, 13^{51}, 2^{191}, 1249^{19}, 248461^{11}, 2^{199}, 411484343^{7}, 2^{203}, 2^{207}, 2^{211}, 2^{213}, 2^{217}, 5^{95}, 2^{221}, 2^{225}, 3^{143}, 7^{81}, 131^{33}, 7^{83}, 13^{63}, 3^{149}, 2^{237}, 3^{151}, 2^{241}, 3^{153}, 2^{243}, 3^{159}, 2^{255}, 7^{91}, 2^{257}, 5^{111}, 2^{259}, 5^{113}, 2^{267}, 2^{271}, 5^{117}, 2^{277}, 3^{177}, 3^{181}, 2^{287}, 2^{293}, 3^{185}, 5^{127}, 2^{295}, 2^{297}, 2^{299}, 3^{191}, 3^{201}, 3^{211}, 5^{145}, 3^{213}, 3^{217}, 3^{219}, 3^{223}, 3^{225}, 3^{227}, and 3^{229}.

Genus 2

- In genus 1, a divisibility check sufficed.
- In genus 2, there are two ways for q to have positive defect.
- The first is through a divisibility condition.
- The second is if q can be represented as a certain polynomial.
- For squares, the only positive defects are $q = 9$ (defect 2) and $q = 4$ (defect 3).
- For non-squares, the positive defects are 1 or 2 (we can distinguish, depending on the size of m.)

Genus 2, odd powers

- The divisibility condition is the same $p|m$ from the genus-1 case.
- The other case is where q is represented by the polynomials x^2+1, x^2+x+1 or x^2+x+2.
- Serre shows the only proper powers represented by those polynomials are $7^3, 2^2, 2^3, 2^5, 2^{13}$.
- So it reduces to the genus-1 search or primes represented by x^2+1 or x^2+x+1.

Genus 2, odd powers

- The second author and Graves computed the first type of primes up to 6.25×10^{28}.
- Preprint on the arXiv as of February 2025: "Primes of the Form $m^2 + 1$ and Goldbach's 'Other Other' Conjecture".
- We are looking at computing the second type.
- The original table was computed by the Italian mathematician Luigi Poletti in 1929.

Genus 3: "the situation is much less good"

- In genus 1 and 2, relatively simple tests sufficed to figure out the defect exactly.
- In genus 3, no such pleasing conditions are known.
- It is not even known whether the defect is bounded in general.
- In Serre's words (conjecture 4.3.1): "Let $m = \lfloor 2q^{1/2} \rfloor$. Then

$$|N_q(3) - (q + 1 + 3m)|$$

  is bounded as q varies (maybe by ≤ 6?)"

Genus 3, minimal relative defect

- However, we can the defect away from the Hasse bound using similar tests.
- Definition: the minimal relative defect (MRD) a is the smallest integer a such that there exists a genus 3 curve $X/\mathbb{F}_q$ with $|\#X(\mathbb{F}_q) - q - 1| = 3m - a$. In particular, $N_q(3) \leq 1 + q + 3m - a$.
- Thus positive a suffices to know that the curve has positive defect (though not what exactly that defect is.)
- There DO exist nice arithmetic tests to compute a! (Lauter 2002)
- e even is boring.
- For e odd:
  - the usual $p|m$ implies positive defect in genus 3 (MRD 2 or 3)
  - $q = x^2 + r$, $r = 1$ or $r = 2$ implies $a = 2$
  - $q = x^2 + x + r$, $r = 1$ or $r = 3$ implies $a = 3$
  - Generalizing the G/Graves sieve code to prime powers of this forms is another next step.

Genus > 3

- ???????
- Let's play a game of wildly speculative pattern matching.
- Sufficient conditions for a curve to have positive defect:
  - Genus 1: $p|m$
  - Genus 2: $p|m$, or q representable by x^2+1, x^2+x+1, x^2+x+2
  - Genus 3: $p|m$, or q representable by x^2+1, x^2+x+1, x^2+2, x^2+x+3
- Can you get sufficient conditions in higher genus when q is representable by some wider set (say, of size $g+1$) polynomials?

Future work

- Extend computations to bigger bounds.
- Computations of Poletti primes.
- Decide when this becomes a paper.