EXHAUSTIVE SEARCH FOR TORSORS OVER $\mathbb{F}_p(t)$

SUNITA BHATTACHARYA

Abstract. Working over global function fields, $\mathbb{F}_p(t)$, we searched for equations of all possible degree 2 genus one curves with a fixed Jacobian and with definite bounds on the degree of the coefficients at different primes. Given a prime p, we try to establish a bound on the number of curves we can find given particular coefficients for a given function field.

1. Introduction

Given a prime p, we consider the global function field $\mathbb{F}_p(t)$, the field of rational functions in one variable, x over a finite field of p elements. We then use these functions as coefficients to construct the degree two genus one curve, the Jacobian, $Jac(C)$ of which is isomorphic to an elliptic curve, E over the field K. After putting a condition on the coefficients of Elliptic curve, we find the other coefficients for the genus one curve, which is a torsor of E.

2. Background

An Elliptic curve is both a curve and a group and is given by $y^2 = x^3 + fx + g$ where, $f, g \in \mathbb{F}_p(t)$. We give few relevant definitions below.

Definition 2.1. A (degree 2) genus one curve is the set of solutions of an equation of the form:

$$w^2 = q(u, v)$$

$$w^2 = au^4 + bu^3v + cu^2v^2 + duv^3 + ev^4$$

where q is a homogenous quartic, $u, v, w \in$ field K and at least one of $u, v \neq 0$

We say that another genus one curve C' is isomorphic to C if the corresponding quartics are equivalent.

2010 *Mathematics Subject Classification.* 14H57; 11G07.
Supported by NSF Grant 1850663.
Communicated by ...

Definition 2.2. Torsors of an Elliptic curve - Let E/K be an Elliptic curve. Also called the Principal Homogenous Space, a torsor of an Elliptic curve is a pair (C, μ), where C is a genus one curve and μ is a simply transitive group action such that

$$\mu : E(\bar{K}) \times C(\bar{K}) \to C(\bar{K})$$

The Trivial torsor is $(E, +)$ with the addition map. A torsor is given in the following form:

$$w^2 = au^4 + bu^3 + cu^2 + du + e$$

Trivially, an Elliptic curve is a torsor of itself.

Tom Fisher[2] gives an explicit formula for the Jacobian of genus one curve, C:

$$y^2 = x^3 + cx^2 - 4aex - 4ace + ad^2$$

A change of variable from x to $x - \frac{c}{3}$ gives us the following standard form:

$$y^2 = x^3 - \frac{12ae + c^2}{3}x + ad^2 - \frac{8ace}{3} + \frac{2c^3}{27}$$

This gives us the following f, g

$$f = -\frac{12ae + c^2}{3}$$

$$g = ad^2 - \frac{8ace}{3} + \frac{2c^3}{27}$$

For a non-trivial torsor C of E, the coefficients satisfy $ad^2 = c^3 + fc + g$ for polynomials $a(t), c(t), d(t)$

The map from the equation:

$$w^2 = au^4 + cu^2 + du + e$$

to points on the curve:

$$ay^2 = x^3 + fx + g$$

is a bijection. By the knowledge of a, c, d and $b = 0$, e is determined. Since $f = -\frac{12ae+c^2}{3}$, we can find $e = -\frac{3f+c^2}{12a}$

Thereby, we have all the coefficients for a torsor we're interested in.

3. Exhaustive algorithm

As we tend to do an exhaustive search for torsors over $F_p(t)$, we work with irreducible polynomials f, g which are not necessarily monic. This code for this algorithm can be found at Github[1]. We want to understand the number of c that satisfy the following conditions :-

- So that d is a non-unit, discriminant of $c^3 + fc + g = 0$
- So that e is a polynomial, a must divide $c^2 + 3f$

Data: prime p
Result: prints possible number of c in a list
make three lists of all irreducible f, g and c ;
keep a counter variable for all possible c ;
for *search through all irreducible* f **do**
  pass on this f to next steps ;
  for *search through all irreducible* g **do**
    take out the g and work with the f from the outer loop ;
    create a list of c such that the $\text{disc}(c^3 + fc + g) = 0$;
    for *loop through all* c **do**
      factor out $c^3 + fc + g$ in the form of ad^2 ;
      if $a|c^2 + 3f$ *is true* **then**
        add c to the list that satisfies two conditions ;
        add to counter variable ;
      end
      print the number of values of c for the particular run ;
    end
  end
  print counter variable (gives the number of all f, g and c for the prime we work at) ;
end

Algorithm 1: Exhaustive Algorithm

4. Results and Examples

We propose the following definitions and conjecture about the results obtained.

Definition 4.1. $n(p)_{(f,g)}$ The number of c that are found for a given f, g at prime p

Definition 4.2. $m(p)$ The maximum number of c that can be found for a given f, g at prime p. This is also the maximum of all $n(p)_{(f,g)}$

We have been interested in finding a bound for $m(p)$. Since, we have worked on finite fields, $m(p)$ is surely finite. Below is a table of $m(p)$ vs. p

p	$m(p)$
2	0
3	0
5	4
7	7
11	7
13	8
17	8

There's no definite pattern in the values of $m(p)$ that came up through Sage calculation but we did conjecture the following for primes less or equal to 17:

$$m(p) <= p$$

We have run the code more than once to test it's reliability. It takes quite a while to check through all the possible combinations. For example, at prime 13, we had 936 irreducible f and 8736 irreducible g to check and that brings to checking just about $8,176,896$ cases. We even analysed the number of c by seeing its frequency. Below is a table for the prime 11.

Number of c	Frequency
$7 = m(11)$	2200
6	7700
5	9900
4	58960
3	157575
2	494420
1	449190

Example 4.1. $f = 6t^2+10t+6$ and $g = 5t^3+6t^2+3t+9$ All the c that satisfy the two conditions are - $t+9, 4t+9, 4t+10, 9t+2, 10t+4$ so here, $n(11)_{(f,g)} = 5$ which is obviously less than $m(11)$ Below is a table of c with the corresponding values of a and d.

c(t)	a(t)	d(t)
t+9	t	t+10
4t+9	5t+15	t
4t+10	5t+30	t+5
9t+2	7t+35	t+3
10t+4	9t+81	t+4

Example 4.2. $f = 2t^2 + 9t + 6$ and $g = 4t^3 + 4t^2 + t + 10$

All the c that satisfy are - 3t + 7, 4t + 9, 5t + 5, 6t + 1, 10t + 4, 10t + 7. Again, we have $n(11)_{f,g} = 6 \leqslant m(11) = 7$. We give the following chart like the previous etample below.

c(t)	a(t)	d(t)
3t + 7	4t+8	t+9
4t+9	10t+20	t+7
5t+5	7t+49	t
6t+1	t+7	t+9
10t+4	t+8	t+9
10t+7	t+7	t+6

Example 4.3. In this example we don't know the value of $m(23)$. We only know about $n(23)_{(f,g)}$ $f = 19t^2 + 7t + 7$ *and* $g = 17t^3 + 16t^2 + 13t + 3$

Here, $n(23)_{(f.g)} = 3$

c(t)	a(t)	d(t)
3t+8	t+17	t+14
6t+22	2t+36	t+14
21t + 16	17t+323	t+18

5. Conclusions and Open Questions

The total number of torsors one could find over $\mathbb{F}_p(t)$ is finite. What we can guarantee is given any f and g in one of the fields we have check, we can't find more than $m_(p)$ that give rise rise to the equation of the torsors. Due to lack of time and computational opportunities, we could not go beyond prime 17. As we increase the prime, the number of cases we need to check increases drastically and the code takes several hours to finish running. Below are a few questions that we have, are unsolved.

- Why is it that $m(p) \leqslant p$ for all primes less or equal to 17?
- Is it true for primes larger than 17 that $m(p) \leqslant p$?
- So far the sequence of $m(p)$ has been an increasing sequence. Is it going to be true for all primes that $m(p_2) \geqslant m(p_1)$ if $p_2 > p_1$?

References

[1] Sunita Bhattacharya. *SageMath Code*. 2019. URL: https://github.com/sunitab55/world-hello.

[2] Tom Fisher. "On some algebras associated to genus one curves". In: *J. Algebra* 518 (2019), pp. 519–541. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2018.09.011. URL: https://doi.org/10.1016/j.jalgebra.2018.09.011.

[3] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd. Springer-Verlag fffdfffdfffd Graduate Texts in Mathematics, 2009. ISBN: 978-0-387-09493-9. URL: http://www.math.brown.edu/~jhs/AECHome.html.

Department of Mathematics, University of California Santa Barbara, Santa Barbara, United States

E-mail address: sunitabhatta@umass.edu