The circle equation over finite fields

Aabrandt, Andreas; Hansen, Vagn Lundsgaard

Published in:
Quaestiones Mathematicae

Link to article, DOI:
10.2989/16073606.2017.1395774

Publication date:
2018

Document Version
Peer reviewed version

THE CIRCLE EQUATION OVER FINITE FIELDS

ANDREAS AABRANDT AND VAGN LUNDSGAARD HANSEN

Abstract. Interesting patterns in the geometry of a plane algebraic curve C can be observed when the defining polynomial equation is solved over the family of finite fields. In this paper, we examine the case of C the classical unit circle defined by the circle equation $x^2 + y^2 = 1$. As a main result, we establish a concise formula for the number of solutions to the circle equation over an arbitrary finite field. We also provide criteria for the existence of diagonal solutions to the circle equation. Finally, we give a precise description of how the number of solutions to the circle equation over a prime field grows as a function of the prime.

Subject class: 11G20, 11D45, 11A07, 14G15
Keywords: Diophantine geometry, prime numbers, siamese twin primes

1. Introduction

From ancient time, shapes and numbers have been fundamental objects for organizing any kind of civilization, and the birth of mathematics is intimately related to exploring these objects. In the Greek culture, studies of shapes and numbers went hand in hand and culminated in work of Diophantus in the third century. Diophantus has lent his name to *diophantine geometry*, which is the study of geometrical properties of the set of solutions to polynomial equations over integers, rational numbers and more general number fields.

The fundamental work *Disquisitiones Aritmeticae* published by Gauss in 1801 marked a new era for the theory of numbers; see Kline [4]. Gauss introduced and made systematically use of the notion of congruence of numbers to solve algebraic equations modulo a prime number, i.e. solving the equations over a prime field. With the path breaking work of Abel and Galois in the 1820s on solutions to polynomial equations, permutation groups and finite fields composed of roots to such equations came into focus. Out of this, diophantine geometry over finite fields emerged as an important research area. In the second half of the twentieth century the subject flourished. It began with the inspired survey paper on the number of solutions of equations in finite fields published 1949 by André Weil [7], in which the four famous conjectures, known as the Weil conjectures, were formulated. The last one of the Weil conjectures was resolved in 1973 by Pierre Deligne [2], a merit rewarded with the Abel Prize in 2013.

In this paper we address some questions in diophantine geometry over finite fields which appear not to have been fully explored.

Consider a plane algebraic curve C over the real numbers given as the solution set to a polynomial equation in two real variables x and y with integer coefficients.

The questions concern what remains of C, when we solve the equation over a finite field. Specifically, we study among others the following questions:

- How does the solution set change when the underlying equation is solved over a finite field?
- How does the number of solutions change with the order of the finite field?

The questions can be posed for any choice of C. To obtain specific results we need, however, to make a specific choice. In this paper we shall examine the case of C being the unit circle defined by the circle equation

$$x^2 + y^2 = 1.$$

The paper opens with a detailed study of the circle equation over the finite field $\mathbb{F}_p$ of prime order p, and more generally over the finite field $\mathbb{F}_{p^n}$ of order p^n for any natural number $n \in \mathbb{N}$. In the main Theorem 3.1 we prove that the number of solutions N_{p^n} to the circle equation over the finite field $\mathbb{F}_{p^n}$ is given by the formula

$$N_{p^n} = p^n - \sin\left(p^n \frac{\pi}{2}\right).$$

We are aware that our formula for the number of solutions to the circle equation over finite fields can be extracted from results in [6] after some nontrivial work.

Using the formula for the number of solutions to the circle equation over a finite field $\mathbb{F}_{p^n}$, we next make a study of how the number of solutions behave as a function of p^n. In Theorem 4.2 we settle the question when the circle equation over any finite field has diagonal solutions, i.e. solutions of the form $(x, y) = (x, x)$. For the prime fields $\mathbb{F}_p$ we obtain in Theorem 4.3 a very precise answer to the question how the number N_p of solutions to the circle equation over $\mathbb{F}_p$ grows as a function of p. Certain pairs of twin primes, which we term *siamese twin primes*, play a surprising role.

2. Some basic results

Since a finite field of characteristic p has order p^n for some $n \in \mathbb{N}$, only finite fields of characteristic 2 can have even order. The following theorem contains therefore, in particular, the complete answer to the question about the number of solutions to the circle equation over a finite field of even order.

Theorem 2.1. *Over the finite field $\mathbb{F}_{p^n}$ corresponding to the prime p and the integer $n \geq 1$, the equation*

$$x^{p^k} + y^{p^k} = 1$$

has exactly p^n solutions of ordered pairs (x, y) of elements $x, y \in \mathbb{F}_{p^n}$ for any integer $k \geq 1$.

Proof. Let $k \geq 1$ be an arbitrary integer. By rewriting the binomial coefficient

$$\binom{p^k}{r} = \frac{p^k!}{r!(p^k - r)!}, \quad 1 \leq r \leq p^k - 1,$$

we get

$$p^k! = \binom{p^k}{r} r!(p^k - r)! \, .$$

Making use of uniqueness of prime factorization, it is easily seen that p^k is a factor in $\binom{p^k}{r}$, and hence that $\binom{p^k}{r} = 0$ in $\mathbb{F}_{p^n}$. By the binomial formula we get then

$$(x + y)^{p^k} = x^{p^k} + y^{p^k}.$$

Together with the obvious relation

$$(xy)^{p^k} = x^{p^k} y^{p^k},$$

this proves that the power map $x^{p^k} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defines an isomorphism of the finite field $\mathbb{F}_{p^n}$ onto itself.

From this follows immediately that

$$(x + y)^{p^k} = 1 \quad \text{if and only if} \quad x + y = 1.$$

Clearly this implies that for every one of the p^n elements $x \in \mathbb{F}_{p^n}$, there exists a unique element $y \in \mathbb{F}_{p^n}$ such that

$$x^{p^k} + y^{p^k} = (x + y)^{p^k} = 1.$$

This proves that the equation $x^{p^k} + y^{p^k} = 1$ has exactly p^n solutions. □

Remark. There are p^{2n} ordered pairs (x, y) of elements in $\mathbb{F}_{p^n}$ and of these only p^n satisfy the equation $x^p + y^p = 1$.

The following special case of Theorem 2.1 provides as mentioned the number of solutions to the circle equation over all finite fields of even order.

Corollary 2.1. *Over the finite field $\mathbb{F}_{2^n}$ corresponding to the prime 2 and the integer $n \geq 1$, the circle equation*

$$x^2 + y^2 = 1$$

has exactly 2^n solutions of ordered pairs (x, y) of elements $x, y \in \mathbb{F}_{2^n}$.

Further on the number of solutions to the circle equation over $\mathbb{F}_p$ we have the following result.

Theorem 2.2. *Solutions to the circle equation*

$$x^2 + y^2 = 1$$

over the finite field $\mathbb{F}_p$ for p odd comes in multiples of four.

Proof. For any odd prime p, you always have the four solutions $(1, 0)$, $(0, 1)$, $(p-1, 0)$ and $(0, p-1)$. Suppose now that $(x, y) = (a, b)$, $1 \leq a, b \leq (p-1)/2$, is a solution. Then $(a, -b) = (a, p - b)$, $(-a, b) = (p - a, b)$ and $(-a, -b) = (p - a, p - b)$ are also solutions. This completes the proof. □

In the table below, we display for each of the primes $p = 2, 3, 5, 7, 11, 13$, the set of all ordered pairs (x, y) of elements in the prime field $\mathbb{F}_p$ that constitutes the set of solutions and the number N_p of solutions to the circle equation over $\mathbb{F}_p$.

TABLE 1. Solutions for $p = 2, 3, 5, 7, 11, 13$.

p	Solutions to $x^2 + y^2 = 1$	N_p
2	$(0,1), (1,0)$	2
3	$(0,1), (1,0), (0,2), (2,0)$	4
5	$(0,1), (1,0), (0,4), (4,0)$	4
7	$(0,1)$,$(0,6)$,$(1,0)$,$(2,2)$,$(2,5)$,$(5,2)$,$(5,5)$,$(6,0)$	8
11	$(0,1), (0,10), (1,0)$,$(3,5), (3,6), (5,3)$, $(5,8)$,$(6,3), (6,8), (8,5), (8,6), (10,0)$	12
13	$(0,1), (0,12), (1,0), (2,6), (2,7), (6,2)$, $(6,11), (7,2), (7,11), (11,6), (11,7), (12,0)$	12

3. Solutions to the circle equation over a finite field

In this section we extend the result for the prime 2 in Corollary 2.1 to include also the odd primes. The formula we present in Theorem 3.1 for the number of solutions to the circle equation over a finite field of odd characteristic can with some work be deduced from more general results on solutions to quadratic forms over finite fields developed by Lidl and Niederreiter in [6]. We offer, however, a self-contained direct proof of the formula.

Theorem 3.1. *For any finite field $\mathbb{F}_{p^n}$ of characteristic p, the number of solutions to the circle equation*

$$x^2 + y^2 = 1$$

over $\mathbb{F}_{p^n}$ is given by the formula

$$N_{p^n} = p^n - \sin\left(p^n \frac{\pi}{2}\right).$$

Proof. For $p = 2$ the result follows by Corollary 2.1. Hence it only remains to consider the case for an odd prime p. For convenience put $q = p^n$.

The multiplicative group $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, say generated by the element $g \in \mathbb{F}_q^*$, see [5]. Every element in $\mathbb{F}_q^*$ is then uniquely presented as a power g^k of g, where the exponent k is counted modulo q.

We define the multiplicative homomorphism $\eta : \mathbb{F}_q^* \to \mathbb{S}$ of $\mathbb{F}_q^*$ onto the multiplicative group $\mathbb{S} = \{-1, 1\}$, by setting $\eta(c) = (-1)^k$, for $c = g^k \in \mathbb{F}_q^*$.

In the literature η is known as the *quadratic character* of $\mathbb{F}_q^*$. For convenience we set $\eta(0) = 0$.

The squaring homomorphism $x^2 : \mathbb{F}_q^* \to \mathbb{F}_q^*$ maps the element $a = g^l \in \mathbb{F}_q^*$ into $c = g^{2l} \in \mathbb{F}_q^*$. From this we conclude that $c = g^k$ is a square in $\mathbb{F}_q^*$ if and only if k is even modulo q, or equivalently, if and only if $\eta(c) = 1$. Hence there are equally many squares and non-squares in $\mathbb{F}_q^*$. From this follows immediately that

$$\sum_{c \in \mathbb{F}_q} \eta(c) = 0.$$

The number of solutions N_q can be decomposed into a sum of products of the number of solutions $N_q(x^2 = c_1)$ and $N_q(y^2 = c_2)$ to the equations $x^2 = c_1$ and $y^2 = c_2$, for $c_1, c_2 \in \mathbb{F}_q$ with $c_1 + c_2 = 1$. Precisely

$$N_q = \sum_{c_1+c_2=1} N_q(x^2 = c_1) N_q(y^2 = c_2).$$

Observing that the equation $z^2 = c$ over $\mathbb{F}_q^*$ has exactly two solutions if any, the expression for N_q can be rewritten as follows using the quadratic character

$$\begin{aligned} N_q &= \sum_{c_1+c_2=1} [1 + \eta(c_1)]\,[1 + \eta(c_2)] \\ &= \sum_{c_1+c_2=1} [1 + \eta(c_1) + \eta(c_2) + \eta(c_1)\eta(c_2)] \\ &= q + \sum_{c_1 \in \mathbb{F}_q} \eta(c_1) + \sum_{c_2 \in \mathbb{F}_q} \eta(c_2) + \sum_{c_1+c_2=1} \eta(c_1 c_2) \\ &= q + \sum_{c \in \mathbb{F}_q} \eta\left(c(1-c)\right). \end{aligned}$$

Now using that $\eta(4) = \eta(2^2) = 1$ we can further rewrite this as

$$\begin{aligned} N_q &= q + \eta(-1) \sum_{c \in \mathbb{F}_q} \eta(4c^2 - 4c) \\ &= q + \eta(-1) \sum_{c \in \mathbb{F}_q} \eta\left((2c-1)^2 - 1\right) \\ &= q + \eta(-1) \sum_{c \in \mathbb{F}_q} \left(-1 + \left[1 + \eta\left((2c-1)^2 - 1\right)\right]\right) \\ &= q + \eta(-1)(-q) + \eta(-1) \sum_{c \in \mathbb{F}_q} \left[1 + \eta\left((2c-1)^2 - 1\right)\right]. \end{aligned}$$

By definition of the quadratic character η, the sum

$$S = \sum_{c \in \mathbb{F}_q} \left[1 + \eta\left((2c-1)^2 - 1\right)\right]$$

is the number of solutions in $\mathbb{F}_q$ to the quadratic equation

$$(2c-1)^2 - 1 = a^2,$$

which can be rewritten as

$$(2c - 1 + a)(2c - 1 - a) = 1.$$

To solve this product of two linear equations, observe that the factor

$$2c - 1 + a = \alpha$$

can be chosen arbitrarily in $\mathbb{F}_q^*$. Then necessarily

$$2c - 1 - a = \alpha^{-1}.$$

By subtraction of equations and division by 2, we get $a = 2^{-1}\left(\alpha - \alpha^{-1}\right)$.

Inserting this value for a into the expression for α yields

$$c = 2^{-1}\left[\alpha + 1 - 2^{-1}\left(\alpha - \alpha^{-1}\right)\right].$$

Since every solution to the quadratic equation in this way turns out to be uniquely determined by a choice of $\alpha \in \mathbb{F}_q^*$ and since the order of $\mathbb{F}_q^*$ is $q-1$, we conclude that the sum S has the value $S = q - 1$.

Collecting facts we get

$$N_q = q + \eta(-1)(-q) + \eta(-1)(q-1) = q - \eta(-1).$$

Now it only remains to determine the value of η on $-1 \in \mathbb{F}_q^*$, i.e. to determine whether -1 is a square, resp. a non-square in $\mathbb{F}_q^*$.

We can choose a generator g of $\mathbb{F}_q^*$ for which $g^0 = 1$, and $g^0, g^1, \ldots, g^{q-2}$ are all the elements in $\mathbb{F}_q^*$, when counting exponents for g modulo $q-1$.

The odd number $q = p^n$ has a unique representation either as $q = 4k+1$ or $q = 4k+3$, for k a non-negative integer.

Suppose $x = g^l$, $1 \leq l < (p^n - 1)/2$, is an element with $x^2 = g^{2l} = -1$. Then $g^{4l} = g^{2l}g^{2l} = (-1)(-1) = 1 = g^0$. Consequently

$$4l \equiv 0 \pmod{q-1}.$$

Now suppose $q = 4k+1$. Then we look for solutions to the congruence

$$4l \equiv 0 \pmod{4k}.$$

We get a solution if k divides l, and hence solutions always exist. We conclude that -1 is a square in $\mathbb{F}_q^*$ for $q = 4k+1$.

Next suppose $q = 4k+3$. Then we look for solutions to the congruence

$$4l \equiv 0 \pmod{4k+2}.$$

A solution exists only if $2k+1$ divides $2l$. Since the odd number $2k+1$ can never be a proper factor in an even number $2l < 4k+2$, we conclude that the congruence has no solutions and hence that -1 is a non-square in $\mathbb{F}_q^*$ for $q = 4k+3$.

It follows that -1 is a square in $\mathbb{F}_q^*$ if and only if $q \equiv 1 \pmod 4$, and hence

$$\eta(-1) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4, \\ -1 & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

In conclusion we get

$$N_q = q - \sin\left(q\frac{\pi}{2}\right),$$

for any prime p, integer $n \in \mathbb{N}$ and $q = p^n$. □

4. Patterns in the number of solutions to the circle equation

Since we now have the precise number of solutions to the circle equation over $\mathbb{F}_{p^n}$, we can generalize Theorem 2.2 and prove the following.

Theorem 4.1. *Let p be an odd prime and $n \geq 1$ an arbitrary integer. Then the number of solutions to the circle equation $x^2 + y^2 = 1$ over the finite field $\mathbb{F}_{p^n}$ is a multiple of four.*

Proof. The number of solutions is given by

$$N_{p^n} = p^n - \sin\left(p^n\,\frac{\pi}{2}\right).$$

Since p is an odd prime, $p^n \equiv 1 \pmod 4$ or $p^n \equiv 3 \pmod 4$. On the other hand, clearly

$$\sin\left(p^n \frac{\pi}{2}\right) = \begin{cases} 1, & p^n \equiv 1 \pmod 4, \\ -1, & p^n \equiv 3 \pmod 4. \end{cases}$$

It follows that

$$N_{p^n} \equiv 0 \pmod 4.$$

□

The following theorem settles in which finite fields the circle equation has *diagonal solutions*, i.e. solutions of the form $(x, y) = (x, x)$.

Theorem 4.2. *Let p be an odd prime.*

(1) *For an arbitrary integer $n \geq 1$, the circle equation $x^2 + y^2 = 1$ has diagonal solutions over the finite field $\mathbb{F}_{p^n}$ if and only if*

$$2^{(p^n-1)/2} = 1 \text{ in } \mathbb{F}_{p^n}.$$

(2) *There are diagonal solutions to the circle equation over the prime field $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 8$.*

(3) *If there are diagonal solutions to the circle equation over a finite field $\mathbb{F}_{p^n}$, then there are exactly two diagonal solutions.*

(4) *If there are diagonal solutions to the circle equation over the prime field $\mathbb{F}_p$, then there are also diagonal solutions to the circle equation over $\mathbb{F}_{p^n}$ for all $n \geq 1$.*

Proof. Set $q = p^n$.

First suppose that $(x, y) = (a, a)$ is a diagonal solution to the circle equation over the finite field $\mathbb{F}_q$. Then $2a^2 = 1$ and hence $(a^{-1})^2 = 2$, showing that 2 is a square in $\mathbb{F}_q$. Next suppose that 2 is a square in $\mathbb{F}_q$. Then clearly 2^{-1} is also a square in $\mathbb{F}_q$. Therefore there exists an element $a \in \mathbb{F}_q$ such that $a^2 = 2^{-1}$, or equivalently, $a^2 + a^2 = 1$. We conclude that the circle equation has diagonal solutions in the finite field $\mathbb{F}_q$ if and only if 2 is a square in $\mathbb{F}_q$. Notice further that the equation $x^2 = 2^{-1}$ has exactly two solutions $\pm a$, if any, proving part (3) in the theorem.

To finish the proof of part (1) in the theorem, it only remains to determine for which $q = p^n$ the number 2 is a square in $\mathbb{F}_q$.

The finite field $\mathbb{F}_q$ is uniquely determined up to an isomorphism as the splitting field for the polynomial $f(x) = x^q - x$ in the polynomial ring $\mathbb{F}_p[x]$ over $\mathbb{F}_p$, see [5].

From this description follows easily that 2 is a square in $\mathbb{F}_q$ if and only if the polynomial $g(x) = x^2 - 2$ is a divisor in $f(x) = x^q - x$.

By polynomial division in $\mathbb{F}_p[x]$ we get

$$f(x) = x^q - x = h(x)(x^2 - 2) + (2^{(q-1)/2} - 1)x,$$

where

$$h(x) = x^{q-2} + 2x^{q-4} + 2^2 x^{q-6} + \cdots + 2^{(q-3)/2} x.$$

From the above follows immediately that $g(x)$ is a divisor in $f(x)$ and hence that 2 is a square in $\mathbb{F}_q$ if and only if

$$2^{(q-1)/2} = 1 \text{ in } \mathbb{F}_{p^n}.$$

For $n = 1$, i.e. for the prime field $\mathbb{F}_p$, it was known to Gauss (with complete proof) that 2 is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 8$, see e.g. Davenport ([1], page 70). This is part (2) of the theorem.

For an arbitrary integer $n \geq 1$, the prime field $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$. Since the squaring map $x^2 : \mathbb{F}_q^* \to \mathbb{F}_q^*$ is a multiplicative homomorphism mapping $\mathbb{F}_p^*$ into itself, it follows that 2 is a square in $\mathbb{F}_q$ if 2 is a square in $\mathbb{F}_p$.

This proves part (4) and hence completes the proof of the theorem. □

Examples. With reference to Table 1, there are no diagonal solutions to the circle equation over the prime field $\mathbb{F}_p$, for the odd primes $p = 3, 5, 11, 13$, whereas the are two diagonal solutions for the prime $p = 7$.

The finite field $\mathbb{F}_{3^2}$ can be described as the polynomial ring $\mathbb{F}_3[t]$ modulo the irreducible polynomial t^2+1. The nine elements in $\mathbb{F}_{3^2}$ are then uniquely described by the nine polynomials $x = a_0 + a_1 t$, for $a_0, a_1 \in \mathbb{F}_3$. Simple calculations show that $(x, y) = (t, t)$ and $(x, y) = (2t, 2t)$ are the two diagonal solutions to the circle equation over $\mathbb{F}_{3^2}$.

For the number of solutions to the circle equation over a prime field $\mathbb{F}_p$ we can do much better. As we shall see, certain pairs of twin primes, which we term siamese twin primes, turn out to play a special role.

Definition 4.1. A pair of twin primes p and p' for which $p \equiv 3 \pmod 4$ and $p' \equiv 1 \pmod 4$ is called a pair of *siamese twin primes*.

Our main result on the number of solutions to the circle equation in a prime field as a function of the prime can then be given the following concise formulation.

Theorem 4.3. *The number of solutions N_p to the circle equation*

$$x^2 + y^2 = 1$$

over $\mathbb{F}_p$ for odd primes, is a strictly increasing function of p in multiples of four, except in pairs of siamese twin primes p and p', where the function stagnates and $N_p = N_{p'}$.

Proof. Let $p < p'$ be a pair of odd prime numbers. It follows by Theorem 3.1 that $N_{p'} \geq N_p$ and by Theorem 4.1 that $N_{p'} \equiv N_p \pmod 4$.

Now suppose that $N_{p'} = N_p$. Then necessarily p and p' must be a pair of twin primes.

If $p \equiv 1 \pmod 4$ then $p' \equiv 3 \pmod 4$ since $p' = p + 2$, and hence

$$N_{p'} - N_p = p' - p - \sin\left(p'\frac{\pi}{2}\right) + \sin\left(p\frac{\pi}{2}\right) = 4,$$

which contradicts our assumption that $N_p = N_{p'}$.

On the other hand if $p \equiv 3 \pmod 4$ then $p' \equiv 1 \pmod 4$ and hence

$$N_{p'} - N_p = p' - p - \sin\left(p'\frac{\pi}{2}\right) + \sin\left(p\frac{\pi}{2}\right) = 0.$$

Altogether we conclude that $N_{p'} = N_p$ if and only if p and p' is a pair of siamese twin primes. □

It is a famous open question whether there are infinitely many pairs of twin primes. Promising progress has recently been made, e.g., [8] and [3], to settle the question in the affirmative.

If in the end it turns out that there are infinitely many pairs of twin primes, there may, however, still not be infinitely many pairs of siamese twin primes.

Based on computer tests, the present authors believe that there exist an infinite number of pairs of siamese twin primes.

In favour of this conjecture speaks that it is well known, see e.g. [1], that there are infinitely many prime numbers p and p' of each of the two types mentioned in Definition 4.1:

$$p \equiv 3 \pmod 4 \qquad \text{and} \qquad p' \equiv 1 \pmod 4.$$

The conjecture is also supported by the fact that the largest known[1] (at the time of writing) pair of twin primes

$$3756801695685 \cdot 2^{666669} - 1 \quad \text{and} \quad 3756801695685 \cdot 2^{666669} + 1$$

is also a pair of siamese twin primes, i.e.

$$N_{3756801695685 \cdot 2^{666669}-1} = N_{3756801695685 \cdot 2^{666669}+1}.$$

Although it is fairly easy on a modern computer to determine if a given pair of twin primes is a pair of siamese primes, it is not easy to determine how many pairs of siamese twins there exist below a given large number, say below

$$3756801695685 \cdot 2^{666669} + 1.$$

Denote by S_n the number of siamese twin primes below n. Likewise denote by T_n the number of twin primes below n. Then we conjecture that

$$\lim_{n\to\infty} \frac{T_n}{S_n} = 2.$$

The conjecture is supported by computer experiments with primes below $n = 2 \cdot 10^9$, for which number there are 6388041 pairs of twin primes and 3193559 pairs of siamese twin primes below n.

References

[1] Harold Davenport. The Higher Arithmetic. An Introduction to the Theory of Numbers. Dover Publications, Inc., New York, 1983.

[2] Pierre Deligne. La conjecture de Weil. I.. Publ. Math., Inst. Hautes Étud. Sci., 43:273-307, 1973.

[3] Daniel Alan Goldston and János Pintz and Cem Yalçin Yildirim. Primes in tuples IV: Density of small gaps between consecutive primes. Acta Arithmetica, 160(1):37-53, 2013.

[4] Morris Kline. Mathematical Thought from Ancient to Modern Times. Oxford University Press, 1972.

[5] Serge Lang. Algebra. Springer, 2005.

[6] Rudolf Lidl and Harald Niederreiter. Finite Fields. Cambridge University Press, 1997.

[7] André Weil. Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc., 55:497-508, 1949.

[8] Yitang Zhang. Bounded Gaps Between Primes. Annals of Mathematics, 179(3):1121-1174, 2014.

Technical University of Denmark

[1] http://primes.utm.edu/top20/page.php?id=1#records