

The Carlitz group of the rationals

September 11, 2018

Alain Connes

To the memory of David Goss, a great number theorist friend.

Abstract

This paper contains two parts. The first is the solution of a challenge question, proposed by Etienne Ghys, on the determination of all maps from rational numbers to themselves such that the difference quotient $(f(x)-f(y))/(x-y)$ is always a square. The second is the computer determination, done with the help of Stephane Gaubert, of a function of primes which plays a key role in the first part as a generalization of a result of Carlitz.

1 Introduction

Let K be a field and $G(K)$ be the group, which we call the Carlitz group of K , of all bijections $f : K \rightarrow K$ which fulfill the following condition

$$\frac{f(x) - f(y)}{x - y} \in K^2, \quad \forall x \neq y \in K \quad (1)$$

These bijections form a group under composition. This group is the group of all bijections when K is algebraically closed or when it is a perfect field of characteristic two. When $K = \mathbb{R}$ it is the group of orientation preserving homeomorphisms of the line. For finite fields of odd characteristic it was determined by Carlitz [1] as the semi-direct product of the affine group by the Frobenius automorphisms, a group already considered by Galois in his work on primitive solvable equations.

We consider the following very intriguing question formulated by Etienne Ghys¹

Question 1.1. (*E. Ghys*) Determine $G(\mathbb{Q})$.

¹as a challenge during a meeting of the French Academy of Sciences

Our main result is to determine all maps $f : \mathbb{Q} \rightarrow \mathbb{Q}$ such that the following holds

$$\frac{f(x) - f(y)}{x - y} \in \mathbb{Q}^2, \quad \forall x \neq y \quad (2)$$

The answer is given by the following Theorem:

Theorem 1.2. *A map $f : \mathbb{Q} \rightarrow \mathbb{Q}$, fulfills (2) if and only if it is an affine map, $f(x) = a^2x + b$.*

In order to prove Theorem 1.2 we first refine the result of Carlitz for finite fields of odd characteristic by showing (Theorem 2.2 below) that a self-map of \mathbb{F}_q which fulfills (1) is either constant or bijective. As a corollary of this preliminary result we get the *simplicity* of the Paley graphs. The notion of simplicity for a graph is straightforward (see Definition 2.3 below). We then focus in §2.2 on sequences of rational numbers and show that if $f : \mathbb{N} \rightarrow \mathbb{Q}$ is such that (2) holds for $x \neq y \in \mathbb{N}$ and that $f(0) = 0, f(1) = 1$, then $f(j) = j$ for all $j \in \mathbb{N}$. With this at hand one easily gets the Theorem 1.2.

The second part of the paper (§3) is based on extensive computations done in collaboration with Stephane Gaubert and we are indebted to him for his great help. It deals with a quantitative form of Theorem 2.2. Our result on infinite sequences of rational numbers does not exclude the existence of arbitrarily long finite sequences of rational numbers which fulfill the same conditions. This leads one to study for each (odd) prime p the function $L(p)$ which associates to the prime p the smallest number L such that $f(j) = j$ is the only solution of

$$f(0) = 0, f(1) = 1, \frac{f(x) - f(y)}{x - y} \in \mathbb{F}_p^2, \quad \forall x \neq y \in \{0, \dots, L\}$$

In fact we consider the function of two variables $W(p, L)$ (where p is an odd prime and $L < p$ an integer), which gives the number of solutions of the above equation. We give a simple Gaussian estimate of $W(p, L)$ in §3.1. We then show in §3.2 that the function $L(p)$ is larger than the function $n(p)$ giving the first quadratic non-residue. In particular known results on the latter show that the growth of $L(p)$ cannot be $O(\log(p))$ in spite of the slow growth of the function $L(p)$ for primes up to $p = 443$. The computation in §3.3 of the function $W(p, x)$ for sufficiently many primes, in order to make educated guesses on its general behavior, was done by heavy use of parallel computations². The results show that the Gaussian estimate is good in many cases but one meets several primes for which the computation of $W(p, L)$ and of $L(p)$ requires much longer than what the Gaussian estimate would suggest. We measure the non-gaussian behavior of such primes by the function $\sigma(p) = \sum \log W(p, k)$ and compare it with the behavior in $(\log p)^3$ given by the Gaussian estimate.

2 The Carlitz group of \mathbb{Q}

We give in this section the proof of Theorem 1.2. We first refine, in §2.1, the result of Carlitz to remove the hypothesis of bijectivity. We then apply this result to sequences of rational numbers in §2.2 and complete the proof of Theorem 1.2 in §2.3.

²The author thanks the Mésocentre Phymath federating the CMAP, CMLS, CPHT and PMC laboratories of École polytechnique, for providing access to the cluster "Hopper" where parallel computation were performed. Thanks also to François Bachelier and to Pieter van Bijnen for their help at an earlier stage of the computations.

2.1 Strengthening of the result of Carlitz

Let p be an odd prime, q a power of p and $\chi : \mathbb{F}_q \rightarrow \{-1, 0, 1\} \subset \mathbb{C}$ denote the quadratic residue character³.

Lemma 2.1. *Let $H \subset \mathbb{F}_q$ be a subset of cardinality > 1 and with non-empty complement.*

(i) *Assume that $\chi(x - y) = \chi(x' - y)$ for all $x, x' \in H$ and $y \notin H$. Then the cardinality of H fulfills $\#H \leq (q - 1)/2$.*

(ii) *Assume that $\#H \leq (q - 1)/2$ then for any pair of distinct elements $u, v \in H$ there exists at least two elements $y \notin H$ such that $\chi(u - y) \neq \chi(v - y)$.*

(iii) *There exists $u, v \in H, y \notin H$ such that $\chi(u - y) \neq \chi(v - y)$.*

Proof. (i) By a translation one can assume that $0 \notin H$. Then $\chi(x) = \chi(x')$ for all $x, x' \in H$, and thus H is contained in one of the halves of the multiplicative group given by squares or non-squares.

(ii) Assume that $\#H \leq (q - 1)/2$ then its complement H^c contains at least $(q - 1)/2 + 1$ elements. Moreover one has the classical formula⁴ ([2], Lemma 2.1)

$$\sum_{z \in \mathbb{F}_q} \chi(u - z)\chi(v - z) = -1$$

The number j of terms equal to -1 in the sum over $z \in H$ is at most $\#H - 2$ since the contributions of $z = u$ and $z = v$ vanish. Let k be the number of terms equal to -1 in the sum over $z \in H^c$. Then one has $j + k$ terms equal to -1 , two equal to zero and $q - (j + k) - 2$ terms equal to 1 thus

$$-(j + k) + (q - (j + k) - 2) = -1 \Rightarrow j + k = (q - 1)/2$$

But one has $j \leq \#H - 2$ and $\#H \leq (q - 1)/2$ thus one gets $k \geq 2$.

(iii) Assume that $\chi(x - y) = \chi(x' - y)$ for all $x, x' \in H$ and $y \notin H$. Then by (i), the cardinality of H fulfills $\#H \leq (q - 1)/2$. Thus (ii) applies and for any pair of distinct elements $u, v \in H$ there exists at least two elements $y \notin H$ such that $\chi(u - y) \neq \chi(v - y)$. Thus one gets a contradiction. \square

Theorem 2.2. *Let q be a power of an odd prime and $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ such that the following holds*

$$\frac{f(x) - f(y)}{x - y} \in \mathbb{F}_q^2, \quad \forall x \neq y \quad (3)$$

then f is an affine map times a power of the Frobenius automorphism. It is either constant or bijective.

Proof. It is enough to show that if f is not constant it is injective since then the result is Carlitz's Theorem [1]. Assume that H is a non-trivial fiber of f so that

$$H = \{u \in \mathbb{F}_q \mid f(u) = a\}, \quad \#H \geq 2, \quad \#H^c > 0$$

³ $\chi : \mathbb{F}_q \rightarrow \mathbb{C}, \chi(a) = 0 \iff a = 0, \chi(ab) = \chi(a)\chi(b), a \in \mathbb{F}_q^2 \iff \chi(a) \neq -1$. When $q = p$ is prime it is the Legendre symbol.

⁴with χ taking values in \mathbb{C}

Let us show that $\chi(x - y) = \chi(x' - y)$ for all $x, x' \in H$ and $y \notin H$. One has

$$f(x) = f(x'), f(x) - f(y) \neq 0, f(x') - f(y) \neq 0$$

and thus (3) in the form

$$\left(\frac{f(x) - f(y)}{x - y} \right) \left(\frac{f(x') - f(y)}{x' - y} \right) \in \mathbb{F}_q^2$$

implies

$$(x - y)(x' - y) \in \mathbb{F}_q^2$$

which in turns means that $\chi(x - y) = \chi(x' - y)$. We can thus apply Lemma 2.1 and get a contradiction. \square

To state the geometric corollary of Theorem 2.2 for the Paley graphs, we introduce the following notion of simplicity for graphs:

Definition 2.3. (i) An equivalence relation \mathcal{R} on the vertices of a graph Γ is a Γ -congruence if and only if for two distinct \mathcal{R} -classes C, C' the fact that (x, x') is or is not an edge is independent of the choices of $x \in C$ and $x' \in C'$.

(ii) A graph Γ is simple if and only if the only Γ -congruence are the two trivial ones⁵.

When q is a power of an odd prime, and is congruent to 1 modulo 4 one defines the Paley graph $\Gamma(q)$ as the graph with set of vertices $V = \mathbb{F}_q$ and where two vertices x, y are adjacent if and only if $\chi(x - y) = 1$.

Corollary 2.4. The Paley graphs are simple.

Proof. Let \mathcal{R} be a $\Gamma(q)$ -congruence. Choose a section $C \mapsto a(C) \in C$ i.e. an element in each equivalence class. Let $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ be the projection $f(x) := a(C(x))$. Let us show that (3) holds. For $x, x' \in \mathbb{F}_q$, either $f(x) = f(x')$ and (3) holds or the \mathcal{R} -classes C, C' of x, x' are distinct. In that case the fact that (x, x') is or is not an edge is independent of the choices of $x \in C$ and $x' \in C'$ and we can thus choose the elements $a(C)$ and $a(C')$. This shows that $\chi(x - x') = \chi(f(x) - f(x'))$ and hence that (3) holds. Applying Theorem 2.2 to f one gets the simplicity of $\Gamma(q)$. \square

2.2 Sequences of rationals

The problem for \mathbb{Q} gives the following question : study all sequences $f(j) \in \mathbb{Q}, j \in \mathbb{N}$ such that

$$\frac{f(i) - f(j)}{i - j} \in \mathbb{Q}^2, \quad \forall i \neq j \tag{4}$$

Let $\rho_p : \mathbb{Z}_{(p)} \rightarrow \mathbb{F}_p$ be the morphism from the ring $\mathbb{Z}_{(p)}$ of fractions with denominator prime to p to the quotient by the ideal generated by p .

Lemma 2.5. Let p be a prime. Let $f(j) \in \mathbb{Q}, j \in \{0, \dots, p - 1\}$ such that (4) holds for all pairs $i \neq j \in \{0, \dots, p - 1\}$. Assume that the denominators of the $f(j)$ are not divisible by p for $j < p$. Then the map $j \mapsto \rho_p(f(j)) \in \mathbb{F}_p, j < p$, is a self-map of \mathbb{F}_p which fulfills (3).

⁵the diagonal and the coarse one

Proof. Since $f(j) \in \mathbb{Z}_{(p)}$ for $j < p$ one gets for $i, j \in \{0, \dots, p-1\}$ that $\frac{f(i)-f(j)}{i-j} \in \mathbb{Z}_{(p)}$. An element $z \in \mathbb{Z}_{(p)}$ which is a square in \mathbb{Q} is a square in $\mathbb{Z}_{(p)}$ because squaring doubles the p -adic valuations, and one gets that the p -adic valuation of the rational square root of z is ≥ 0 . It follows that $\frac{f(i)-f(j)}{i-j} \in \mathbb{Z}_{(p)}^2$ and one gets, applying ρ_p that the map $j \mapsto \rho_p(f(j)) \in \mathbb{F}_p$ fulfills (3). \square

Lemma 2.6. *Let $f : \mathbb{N} \rightarrow \mathbb{Z}$ be such that (4) holds and that $f(0) = 0, f(1) = 1$. Then $f(j) = j$ for all $j \in \mathbb{N}$.*

Proof. For each prime p one can consider the map $f_p : \mathbb{F}_p \rightarrow \mathbb{F}_p$ obtained by reducing $f(j)$ modulo p for $0 \leq j < p$. For two distinct elements $0 \leq i < j < p$ one has by hypothesis that $(j-i)(f(j) - f(i))$ is the square of a rational number, and hence the square of an integer. Thus the same holds for f_p and by Theorem 2.2, one has that f_p is the identity. This shows that $f(j) - j$ is divisible by any prime $> j$ and hence is equal to 0. \square

Lemma 2.7. *Let $f : \mathbb{N} \rightarrow \mathbb{Q}$ be such that (4) holds and that $f(0) = 0, f(1) = 1$. Then $f(j) = j$ for all $j \in \mathbb{N}$.*

Proof. Let us look at the denominators which may appear in a sequence $f(j)$ of rational numbers ($j \geq 0$) such that $f(0) = 0, f(1) = 1$ and that (4) holds. For a prime p we look at the first occurrence of a negative power of p in $f(j)$:

$$j_p(f) := \inf\{j \mid \text{Val}_p(f(j)) < 0\} \quad (5)$$

One has $j_p(f) \geq 2$ by construction. Moreover since $\text{Val}_p(f(j_p - 1)) \geq 0$ one has

$$\text{Val}_p(f(j_p)) = \text{Val}_p(f(j_p) - f(j_p - 1)) \in 2\mathbb{Z}$$

since $f(j_p) - f(j_p - 1)$ is a square. In fact one can consider the finite differences

$$\alpha(k) = (f(j_p + k) - f(j_p - 1))/(1 + k), \quad k \in \{0, \dots, p-2\}$$

By hypothesis $\alpha(k)$ are squares in \mathbb{Q} and since $(1+k)$ is prime to p , the p -adic valuation $\text{Val}_p(\alpha(k))$, if it is negative, is the same as $\text{Val}_p(f(j_p + k) - f(j_p - 1))$. It is even since $\alpha(k)$ are squares and thus if $k \in \{0, \dots, p-2\}$ is such that $\text{Val}_p(f(j_p + k)) < 0$ one gets

$$\text{Val}_p(f(j_p + k)) = \text{Val}_p(f(j_p + k) - f(j_p - 1)) \in 2\mathbb{Z}$$

We now consider the interval of length p given by $I_p := \{j_p - 2, \dots, j_p + p - 3\}$ and we assume $p \geq 3$ so that I_p contains j_p . We then define

$$e_p(f) := \inf\{\text{Val}_p(f(j)) \mid j \in I_p\} \quad (6)$$

Since all the numbers $\text{Val}_p(f(j)), j \in I_p$, which are negative are even we get that $e_p(f)$ is even and < 0 . We can thus multiply the $f(j)$ for $j \in I_p$ by $p^{-e_p(f)}$ without altering the fact that the finite differences are squares of rationals. We then consider the map

$$r_p(f)(k) := \rho_p(f(j_p - 2 + k)p^{-e_p(f)}) \in \mathbb{F}_p \quad (7)$$

The map $r_p(f)$ fulfills (3) by Lemma 2.5. It takes the same value 0 at $k \in \{0, 1\}$. This implies, by Theorem 2.2 that it is constant equal to 0 but this gives a contradiction since there exists a non-zero value of $r_p(f)$ due to the definition of $e_p(f)$. Thus we cannot have a non-trivial denominator involving odd primes.

Let us now consider the case $p = 2$. The definition (5) gives an integer j_2 and we assume $j_2 < \infty$. One has $\text{Val}_2(f(j_2)) < 0$. By construction one has $j_2 \geq 2$ and

$$\text{Val}_2(f(j_2 - 2)) \geq 0, \quad \text{Val}_2(f(j_2 - 1)) \geq 0$$

Thus, since $f(j_2) - f(j_2 - 1)$ is a square,

$$\text{Val}_2(f(j_2)) = \text{Val}_2(f(j_2) - f(j_2 - 1)) \in 2\mathbb{Z}$$

But $(f(j_2) - f(j_2 - 2))/2$ is a square and this gives a contradiction since

$$\text{Val}_2((f(j_2) - f(j_2 - 2))/2) = \text{Val}_2(f(j_2) - f(j_2 - 2)) - 1 = \text{Val}_2(f(j_2)) - 1 \in 1 + 2\mathbb{Z}$$

We have shown that no denominator can appear in the sequence $f(j)$ and thus it is integer valued. But then we can apply Lemma 2.6 to get the conclusion. \square

2.3 Proof of Theorem 1.2

By Lemma 2.7 we know that the only sequences $a(n)$, $n \in \mathbb{N}$, of rational numbers, $a(0) = 0$, such that (4) holds are in fact constant times n (and the constant is equal to a square). Indeed either $a(n)$ is constant equal to 0 or there exists a smallest $j_0 > 0$ for which $a(j_0) \neq 0$, but then $a(j_0)$ is a square since $a(j_0 - 1) = 0$ and (4) holds. Thus the sequence $b(u) := a(j_0 + u - 1)/a(j_0)$ fulfills the hypothesis of Lemma 2.7 and is hence equal to u for all $u > 0$. This gives $a(j_0 + u - 1) = ua(j_0)$ for all $u \geq 0$. Let us show that $j_0 = 1$. One has $b(u) = 0$ for $u \in \{-j_0 + 1, \dots, 0\}$ and $b(1) = 1$. Thus if $j_0 \geq 2$, (4) gives that $(b(1) - b(-1))/2$ is a square which is a contradiction. Thus $j_0 = 1$, $a(u) = ua(1)$ for all $u \geq 0$. Let then $f : \mathbb{Q} \rightarrow \mathbb{Q}$ which fulfills (2). One can assume that $f(0) = 0$ by subtracting $f(0)$. Let $x \in \mathbb{Q}$, $x \neq 0$. Let $a(n) := f(nx)/x$. It fulfills the condition (4). Thus we get $a(n) = na(1)$ for all $n \in \mathbb{N}$. This shows that $f(nx)/x = nf(x)/x$ and thus $f(nx) = nf(x)$ for all $n \in \mathbb{N}$. Thus we have for integers $a, b > 0$

$$f(a/b)b = f(a) = af(1) \Rightarrow f(a/b) = a/bf(1) \Rightarrow f(x) = xf(1), \quad \forall x \in \mathbb{Q}_+.$$

This result applies also to the function $g(x) := f(1) - f(1 - x)$ and gives

$$g(x) = xg(1), \forall x \in \mathbb{Q}_+ \Rightarrow f(1) - f(1 - x) = xf(1), \forall x \in \mathbb{Q}_+ \Rightarrow f(1 - x) = (1 - x)f(1), \forall x \in \mathbb{Q}_+.$$

This shows that $f(x) = xf(1)$ for all $x \in \mathbb{Q}$.

3 The minimal length $L(p)$

Theorem 1.2 does not exclude the existence of finite sequences $f(j) \in \mathbb{Q}$, $j \leq L$ such that (4) holds for all pairs $i \neq j \in \{0, \dots, L\}$. For instance one has the following examples of length 4 and 5, i.e. $L = 3$ and $L = 4$,

$$\left\{ 0, 1, \frac{15842}{1681}, 23763 \right\}, \quad \left\{ 0, 1, \frac{2738}{2209}, \frac{3267}{2209}, \frac{5476}{2209} \right\}$$

The above proof of Theorem 1.2 suggests to first control, given a prime p , the possible sequences $f(j) \in \mathbb{F}_p, 0 \leq j \leq L < p$ such that

$$f(0) = 0, f(1) = 1, \frac{f(x) - f(y)}{x - y} \in \mathbb{F}_p^2, \quad \forall x \neq y \in \{0, \dots, L\} \quad (8)$$

By Theorem 2.2 there exists a smallest $L = L(p) < p$ such that the only solution of (8) is $f(j) = j$. We show the graph of the function of n giving the minimal length $L(p(n))$ with $p = p(n)$ the n -th prime. It is shown until $n = 79$ i.e. $p(n) = 401$.

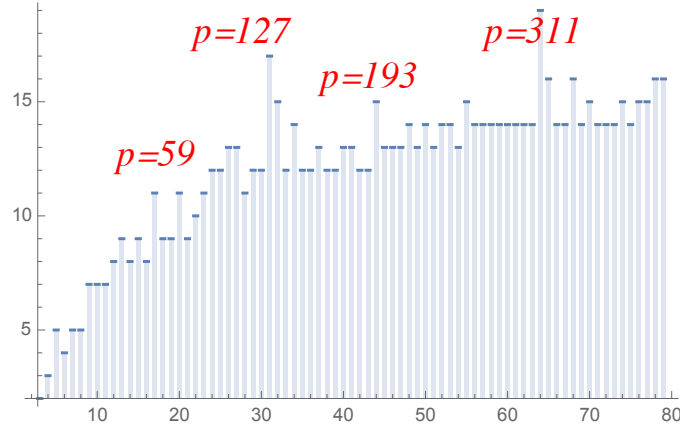


Figure 1: Graph of the function $L(p(n))$ for $5 \leq n \leq 79$.

3.1 Gaussian estimate of the function $W(p, L)$

In order to give an estimate of the order of magnitude of the function $L(p)$ we do a simple counting. In fact we consider the function of two variables $W(p, L)$ where p is an odd prime and $2 \leq L < p$ an integer, which gives the number of solutions of (8). Each time we write that some quantity is a square in \mathbb{F}_p the probability that this is true is the fraction

$$P = \frac{1 + (p - 1)/2}{p} = \frac{p + 1}{2p}$$

When we deal with a list of the form

$$(0, 1, f(2), \dots, f(x))$$

the number of variables is $x - 1$ and the freedom is thus of p^{x-1} . The number of requirements that some expression is a square is

$$S(x) = \sum_{r=2}^x r = \frac{1}{2} (x^2 + x - 2)$$

Thus if we assume the independence at the probabilistic level of the conditions we estimate the number of remaining possibilities as

$$R = p^{S(x)} p^{x-1}.$$

This gives as an approximation for $W(p, L)$ a Gaussian function $G(p, L) = e^{Q(p, L)}$ with exponent the quadratic form, in terms of $L = x$,

$$Q(p, x) = -\frac{1}{2}x^2 \log\left(\frac{2p}{p+1}\right) + \frac{1}{2}x \log\left(\frac{p(p+1)}{2}\right) - \log\left(\frac{p+1}{2}\right)$$

This quadratic form vanishes for $x = 1$ and the other root is thus

$$\ell(p) := 2 \frac{\log(p+1) - \log(2)}{\log(2) - \log(1+1/p)} \sim 2 \frac{\log(p)}{\log(2)}$$

The next lemma shows that the probabilistic estimate is good at the beginning. Indeed for sequences $(0, 1, f(2))$ there are two conditions and they should select about $1/4$ of the possible values of $f(2) \in \mathbb{F}_p$. More precisely one gets:

Lemma 3.1. *Let p be an odd prime. The number of sequences $(0, 1, f(2))$ which fulfill the two conditions $f(2)/2 \in \mathbb{F}_p^2$ and $f(2) - 1 \in \mathbb{F}_p^2$ is equal to $E(p/4) + 1$ where $E(x)$ denotes the integral part of x .*

Proof. We consider the plane curve C defined by the equation $1 + x^2 = 2y^2$. By intersecting the lines through the point $(1, 1)$ we get the rational parametrization: $t \mapsto P(t)$,

$$P(t) := (x, y) = \left(1 - \frac{2(2t-1)}{2t^2-1}, 1 - \frac{2t(2t-1)}{2t^2-1}\right), \quad t = (y-1)/(x-1) \quad (9)$$

For $x = 1$ we have the two points with $y = \pm 1$. For $x \neq 1$ the ratio $t = (y-1)/(x-1)$ is finite and it determines uniquely t and the point $P(t)$. The values of t obtained from $x \neq 1$ are such that $t \neq 1/2$ and $t^2 \neq 1/2$. Moreover for $x = -1$ one gets $t = 0$ and $y = 1$, or $t = 1$ and $y = -1$. But all the 4 points $(\pm 1, \pm 1)$ correspond to the same solution $f(2) = 2$. Thus for the other solutions they correspond to values

$$A_p := \{t \in \mathbb{F}_p \mid t \neq 1/2, t^2 \neq 1/2, t \neq 0, t \neq 1\}$$

The cardinality of A_p is $p - 3$ if 2 is not a square in \mathbb{F}_p and is $p - 5$ otherwise.

The two transformations $\alpha, (x, y) \mapsto (-x, y)$ and $\beta, (x, y) \mapsto (x, -y)$ can now be expressed as the following projective involutions in the variable t , they correspond to the matrices

$$\alpha = \begin{pmatrix} 2 & -1 \\ 2 & -2 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}, \quad \alpha(t) = \frac{2t-1}{2(t-1)}, \quad \beta(t) = \frac{t-1}{2t-1}$$

The fixed points of α are $\left\{t \rightarrow \frac{1}{2}(2 - \sqrt{2})\right\}, \left\{t \rightarrow \frac{1}{2}(\sqrt{2} + 2)\right\}$ which is empty unless 2 is a square. The fixed points of β are $\left\{t \rightarrow \frac{1}{2} - \frac{i}{2}\right\}, \left\{t \rightarrow \frac{1}{2} + \frac{i}{2}\right\}$ which is empty unless -1 is a square. We need to consider 4 cases determined by the residue of p modulo 8.

- $p \equiv 1$ modulo 8. Then both -1 and 2 are squares. Both α and β have two fixed points and thus the number of orbits of the group $H = \mathbb{Z}/4\mathbb{Z}$ acting on A_p is

$$\#A_p/4 + 1 = \frac{p-5}{4} + 1 = \frac{p-1}{4} = E\left(\frac{p}{4}\right)$$

Thus adding the contribution of $(\pm 1, \pm 1)$ one gets the expected result.

- $p \equiv 3$ modulo 8. Then both -1 and 2 are not squares. Both α and β have no fixed points and thus the number of orbits of the group $H = \mathbb{Z}/4\mathbb{Z}$ acting on A_p is

$$\#A_p/4 = \frac{p-3}{4} = E\left(\frac{p}{4}\right)$$

Thus adding the contribution of $(\pm 1, \pm 1)$ one gets the expected result.

- $p \equiv 5$ modulo 8. Then -1 is a square and 2 is not a square. Thus α has no fixed point but β has two fixed points and thus the number of orbits of the group $H = \mathbb{Z}/4\mathbb{Z}$ acting on A_p is

$$(\#A_p - 2)/4 + 1 = \frac{p-5}{4} + 1 = E\left(\frac{p}{4}\right)$$

Thus adding the contribution of $(\pm 1, \pm 1)$ one gets the expected result.

- $p \equiv 7$ modulo 8. Then -1 is not a square and 2 is a square. Thus α has two fixed points but β has no fixed points and thus the number of orbits of the group $H = \mathbb{Z}/4\mathbb{Z}$ acting on A_p is

$$(\#A_p - 2)/4 + 1 = \frac{p-7}{4} + 1 = E\left(\frac{p}{4}\right)$$

Thus adding the contribution of $(\pm 1, \pm 1)$ one gets the expected result.

This shows that in all cases the answer is $E\left(\frac{p}{4}\right) + 1$. □

When we move to the next step *i.e.* sequences of the form $(0, 1, f(2), f(3))$, the probabilistic estimate is still rather good as shown in Figure 2

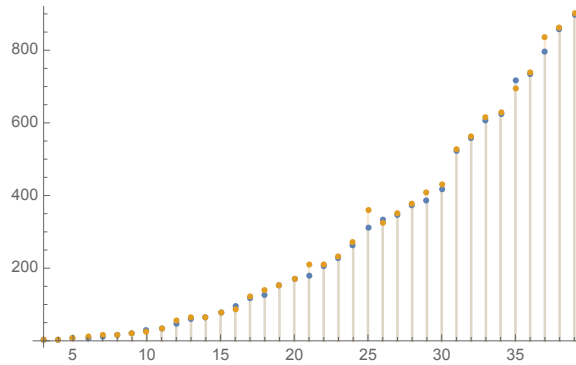


Figure 2: Number of solutions compared to the Gaussian.

In fact the discrepancy is governed by the family of elliptic curves $E(s)$, $v^2 = Q_s(u)$ where

$$Q_s(u) := 4 \left(4s^4 + 16s^3 - 28s^2 + 8s + 1 \right) u^4 - 48 \left(2s^2 - 1 \right)^2 u^3 + 12 \left(36s^4 - 16s^3 - 12s^2 - 8s + 9 \right) u^2 - 72 \left(2s^2 - 1 \right)^2 u + 9 \left(4s^4 + 16s^3 - 28s^2 + 8s + 1 \right)$$

whose discriminant is

$$D(s) = 2^{20} 3^6 (2s^2 - 1)^4 (2s^2 - 4s + 1)^4 (2s^2 - 2s + 1)^4$$

and does not vanish for rational values of s .

Lemma 3.2. *Let $P(s) = (x, y)$ be a point of the curve C of (9) defined by the equation $1 + x^2 = 2y^2$. The sequences $(0, 1, f(2), f(3))$ which fulfill $f(2) = 1 + x^2 = 2y^2$ and the condition $(f(i) - f(j))/(i - j)$ is a square for $i < j, i, j \in \{0, \dots, 3\}$ correspond to the points of the elliptic curve $E(s)$.*

Proof. We consider the two conditions $f(3) - f(0) = 3X^2$ and $f(3) - f(1) = 2Y^2$. This gives the plane curve C' defined by the equation $1 + 2Y^2 = 3X^2$. By intersecting the lines through the point $(1, 1)$ we get the rational parametrization: $u \mapsto R(u)$,

$$R(u) := (X, Y), \quad X = 1 - \frac{2(2u - 3)}{2u^2 - 3}, \quad Y = \frac{2u^2 - 6u + 3}{3 - 2u^2} \quad (10)$$

One then writes the missing equation *i.e.* that $f(3) - f(2)$ is a square. This gives the equation $v^2 = Q_s(u)$ where the polynomial $Q_s(u)$ is determined by the equality

$$f(3) - f(2) = \frac{Q_s(u)}{(2s^2 - 1)^2 (2u^2 - 3)^2}$$

using (9) to input $f(2)$ and (10) to input $f(3)$ as

$$f(2) = \left(1 - \frac{2(2s - 1)}{2s^2 - 1}\right)^2 + 1, \quad f(3) = 3 \left(1 - \frac{2(2u - 3)}{2u^2 - 3}\right)^2$$

Note that in the counting of points of the elliptic curve $E(s)$, the point at ∞ counts 2 because it is a double point. This means that the number of points which are not at ∞ is given by $p - \text{tr}F - 1$ where $\text{tr}F$ is the trace of the Frobenius.

3.2 Lower bound for $L(p)$

Let us define the function $n(p)$ for a prime p as the largest integer $0 \leq n < p$ such that all elements of $\{0, \dots, n - 1\}$ are quadratic residues. In other words $n(p)$ is the first quadratic non-residue.

Lemma 3.3. *Let p be an odd prime. One has $n(p) \leq L(p)$.*

Proof. Consider the sequence given by

$$f(0) = 0, \quad f(u) = 1, \quad \forall u \in \{1, \dots, n(p) - 1\}$$

Let us show that f fulfills (8) for $u, v \in \{1, \dots, n(p) - 1\}$. One can assume that $v = 0$ and $u \neq 0$ since if both u, v are $\neq 0$ (8) is fulfilled since $f(u) = f(v)$. Then $f(u) - f(v) = 1$ and (8) means that u is a quadratic residue, which is true by definition of $n(p)$. Thus as long as $n(p) > 2$ one has a sequence $f(i)$ which fulfills (8) for $i \leq n(p) - 1$ and is not $f(i) = i$, thus $L(p) > n(p) - 1$ and one gets $n(p) \leq L(p)$. \square

p	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
3	5	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	7	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	11	3	6	10	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	13	4	11	17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	17	5	15	29	15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8	19	5	15	33	12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	23	6	21	52	90	42	7	1	1	1	1	1	1	1	1	1	1	1	1	1
10	29	8	25	45	75	117	10	1	1	1	1	1	1	1	1	1	1	1	1	1
11	31	8	36	56	56	28	3	1	1	1	1	1	1	1	1	1	1	1	1	1
12	37	10	55	155	85	57	18	3	1	1	1	1	1	1	1	1	1	1	1	1
13	41	11	63	207	529	1529	616	92	4	1	1	1	1	1	1	1	1	1	1	1
14	43	11	66	248	690	788	166	2	1	1	1	1	1	1	1	1	1	1	1	1
15	47	12	78	312	813	847	266	12	3	1	1	1	1	1	1	1	1	1	1	1
16	53	14	85	265	575	1017	258	3	1	1	1	1	1	1	1	1	1	1	1	1
17	59	15	120	574	1050	810	409	107	32	18	9	1	1	1	1	1	1	1	1	1
18	61	16	139	621	1655	4109	2115	290	3	1	1	1	1	1	1	1	1	1	1	1
19	67	17	153	807	2908	4326	1685	99	9	1	1	1	1	1	1	1	1	1	1	1
20	71	18	171	944	3515	10090	18831	13816	3820	208	5	1	1	1	1	1	1	1	1	1
21	73	19	209	1651	6117	14375	6791	1919	1	1	1	1	1	1	1	1	1	1	1	1
22	79	20	210	954	2368	2932	1676	360	26	6	1	1	1	1	1	1	1	1	1	1
23	83	21	231	1451	6030	10700	12441	13179	18342	23716	379	1	1	1	1	1	1	1	1	1
24	89	23	273	1707	7183	28187	25364	11066	774	12	3	2	1	1	1	1	1	1	1	1
25	97	25	359	3685	15195	37653	22445	10709	7201	8	3	2	1	1	1	1	1	1	1	1
26	101	26	325	2385	10255	30265	70983	144977	269175	343141	7300	161	4	1	1	1	1	1	1	1
27	103	26	351	2121	7077	12131	20426	31580	46109	64592	5120	56	3	1	1	1	1	1	1	1
28	107	27	378	2946	14571	31389	23486	3784	684	59	3	1	1	1	1	1	1	1	1	1
29	109	28	407	2969	11767	36697	88199	139185	195723	264353	10072	34	1	1	1	1	1	1	1	1
30	113	29	429	3333	11449	15630	11306	4042	700	75	10	4	1	1	1	1	1	1	1	1
31	127	32	528	4020	17404	42350	87542	158270	262703	410690	613730	885761	74677	1387	45	9	3	1	1	1
32	131	33	561	5219	21403	39349	42167	21209	5252	786	47	8	4	3	2	1	1	1	1	1
33	137	35	615	5583	23231	37766	39668	20248	5297	552	31	8	1	1	1	1	1	1	1	1
34	139	35	630	6172	25188	44702	47374	28750	9323	1961	267	32	3	2	1	1	1	1	1	1
35	149	38	697	6905	38525	138881	154706	44839	12248	1633	148	5	1	1	1	1	1	1	1	1
36	151	38	741	6743	31424	72926	81047	39200	8470	985	83	10	1	1	1	1	1	1	1	1
37	157	40	835	8805	35921	91131	125956	101503	49464	25542	3602	300	14	1	1	1	1	1	1	1
38	163	41	861	9721	65141	191575	227200	74444	21050	2439	121	6	1	1	1	1	1	1	1	1
39	167	42	903	10428	66519	198627	250421	83981	24519	3352	259	17	1	1	1	1	1	1	1	1
40	173	44	925	9765	57865	219861	618425	1493637	3138025	4160997	129892	2462	6	1	1	1	1	1	1	1
41	179	45	1035	12723	69900	173360	251966	189054	89210	52690	60940	69860	629	1	1	1	1	1	1	1
42	181	46	1091	12991	81715	369071	596594	365810	43296	6585	391	23	1	1	1	1	1	1	1	1
43	191	48	1176	15348	116722	588720	1810128	2540682	1634300	327132	9494	26	1	1	1	1	1	1	1	1
44	193	49	1279	20221	154243	642253	1811389	4020781	7619869	21743809	8337004	1142436	9690	34	4	1	1	1	1	1
45	197	50	1225	16305	118685	529537	804006	375128	97219	15641	1756	174	16	1	1	1	1	1	1	1
46	199	50	1275	15393	95200	294132	461017	353203	21237	2078	152	5	1	1	1	1	1	1	1	1
47	211	53	1431	20471	129716	373031	639897	536759	223648	43190	4764	330	14	1	1	1	1	1	1	1
48	223	56	1596	21672	156408	590702	1604540	3479936	6581035	11350432	2243631	92958	359	2	1	1	1	1	1	1
49	227	57	1653	25293	221115	878931	1776036	2429148	4520370	7253090	770729	345	30	1	1	1	1	1	1	1
50	229	58	1739	26171	208451	1171291	2466742	2216720	491129	112817	12533	746	31	7	1	1	1	1	1	1
51	233	59	1749	26503	190383	596206	1034702	891786	389226	86298	8441	488	9	1	1	1	1	1	1	1
52	239	60	1830	29372	267698	1561616	5510739	9222901	7366619	2007701	94932	404	24	2	1	1	1	1	1	1
53	241	61	1979	38809	546491	6281521	24787263	62936401	124735849	215364097	74367005	27376541	1702999	2	1	1	1	1	1	1
54	251	63	2016	33878	264758	965348	1932458	1872501	894376	220610	24847	1301	40	1	1	1	1	1	1	1
55	257	65	2145	36089	289853	1077046	2414750	2874248	2021505	859823	151420	14679	782	23	3	1	1	1	1	1
56	263	66	2211	38824	363711	1629547	3295318	2188512	1191123	365657	55588	3891	162	7	1	1	1	1	1	1
57	269	68	2257	38405	351135	1901653	7138895	20307973	49251695	75595229	106913095	143176565	6242780	864	1	1	1	1	1	1
58	271	68	2346	38990	326872	1368328	2900734	2911574	1318748	316413	39153	2653	137	11	1	1	1	1	1	1
59	277	70	2495	44615	348973	1544371	3423489	3778726	1982886	534604	72418	5091	169	6	1	1	1	1	1	1
60	281	71	2553	46691	486703	3568771	19503671	86833859	177961341	306872855	53055757	336160	1520	6	1	1	1	1	1	1
61	283	71	2556	48048	504136	2429244	5789040	8422550	16772999	28426344	3845490	1856	51	5	1	1	1	1	1	1
62	293	74	2665	48225	468685	2688993	10354101	31703985	80145925	125119425	10957584	602241	4558	10	1	1	1	1	1	1
63	307	77	3003	60973	686435	3581683	9254016	14144918	28858373	49968934	7388646	7849	352	5	1	1	1	1	1	1
64	311	78	3081	63336	721459	5068694	24887327	94529908	297662793	813717098	1261841916	809829209	279434630	39688205	1438254	6655	39	10	3	1
65	313	79	3259	77491	872947	5134727	10511955	5808647	5078095	657099	85493	5616	292	18	5	2	1	1	1	1
66	317	80	3145	63885	689155	4302789	10447364	8733907	4501510	1218336	153083	10044	333	7	1	1	1	1	1	1
67	331	83	3486	76014	765394	3630036	9569489	12182165	7553884	2199645	300572	20811	877	44	1	1	1	1	1	1
68	337	85	3749	93685	1142877	7272661	28489765	81209509	189599889	616047989	332132160	77738924	1921708	10929	46	2	1	1	1	1
69	347	87	3828	87294	1092195	6377295	17104801	16604851	10709630	3410983	562001	44933	1711	50	1	1	1	1	1	1
70	349	88	3919	87461	995895	6928917	20600076	25074154	8378260	2572656	409481	37102	1698	88	5	1	1	1	1	1
71	353	89	3969	89921	982037	4858382	12482598	16756756	10846844	321918162	4304889	412637	1277	31	1	1	1	1	1	1
72	359	90	4095	96456	1243095	9675762	44337285	99760872	110664637	46947275	4386955	37400	1470	24	1	1	1	1	1	1
73	367	92	4323	97659	1148612	7014776	27303965	77131281	178575509	362373181	119590478	10632066	131691	197	1	1	1	1	1	1
74	373	94	4471	106687	1155807	6861225	20673079</													

On the assumption of the generalized Riemann hypothesis, H. L. Montgomery [4] proved that $n(p) = \Omega(\log p \log \log p)$ i.e. that $\liminf n(p)/(\log p \log \log p) > 0$ and in [3] an unconditional proof was given that $n(p) = \Omega(\log p \log \log \log p)$. Combined with Lemma 3.3 this shows that the asymptotic behavior of the function $L(p)$ is no better than $\log p \log \log \log p$.

3.3 Experimental tests

In collaboration with Stephane Gaubert we computed the functions $W(p, x)$ for all primes up to $p = 443$. We made an arborescent enumeration of the solutions $f(2), \dots, f(L)$, for increasing values of L . Inadmissible sequences were eliminated by a sieve construction. This leads to an algorithm running in time $O(\sum_{2 \leq x \leq L(p)} pxW(p, x))$. The result is given in Table 1.

For the "logarithmic size" i.e. the function $\sigma(p)$,

$$\sigma(p) = \sum_x \log W(p, x),$$

the Gaussian approximation gives the following estimate $g(p)$,

$$g(p) = \frac{\left(2 \log(p) + 3 \log\left(\frac{p+1}{2p}\right)\right)^3}{12 \log^2\left(\frac{p+1}{2p}\right)} \simeq \frac{(2 \log(p) - 3 \log 2)^3}{12 \log^2(2)}$$

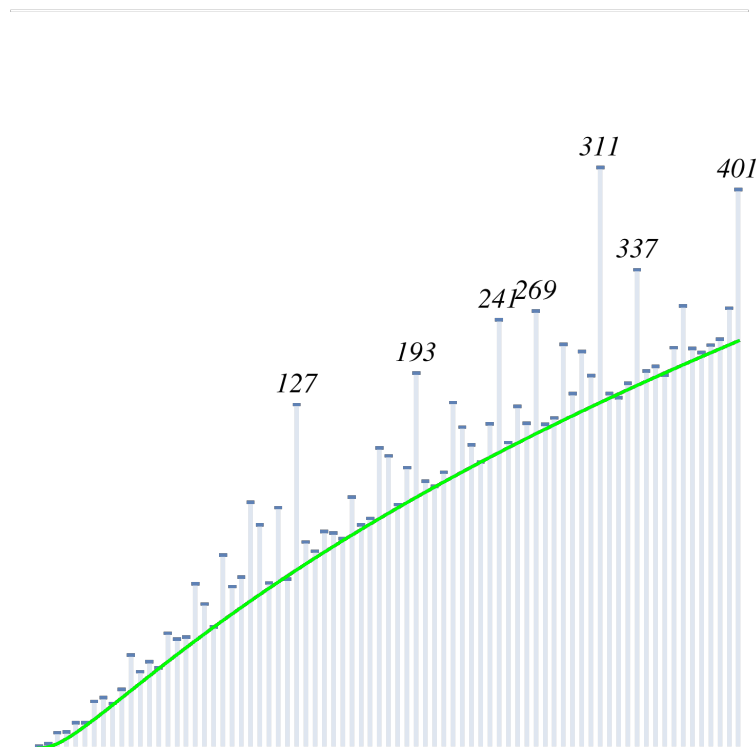


Figure 3: Logarithmic size for $5 \leq n \leq 79$.

Figure 3 shows the graph of $g(p(n))$ in green together with the plot of $\sigma(p(n))$. It shows that there are primes such as $\{101, 127, 193, 241, 269, 311, 337, 401\}$ for which the logarithmic size far exceeds the Gaussian estimate, but that the latter does work in many cases. The next Figure 4 shows the graph of the difference $\sigma(p(n)) - g(p(n))$ up to $n = 79$, i.e. $p(n) = 401$. It is an open challenging question to understand the reason behind these non-Gaussian behaviors.

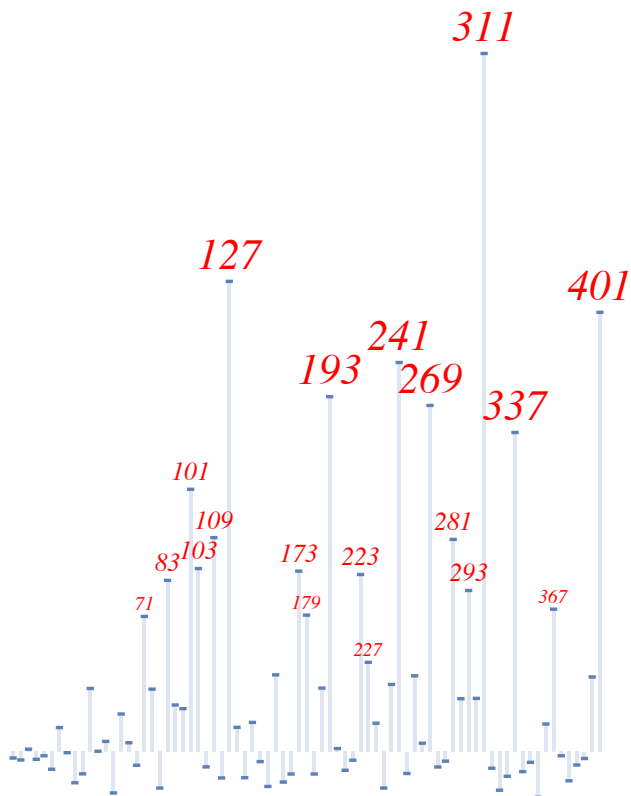


Figure 4: Log discrepancy for $5 \leq n \leq 79$.

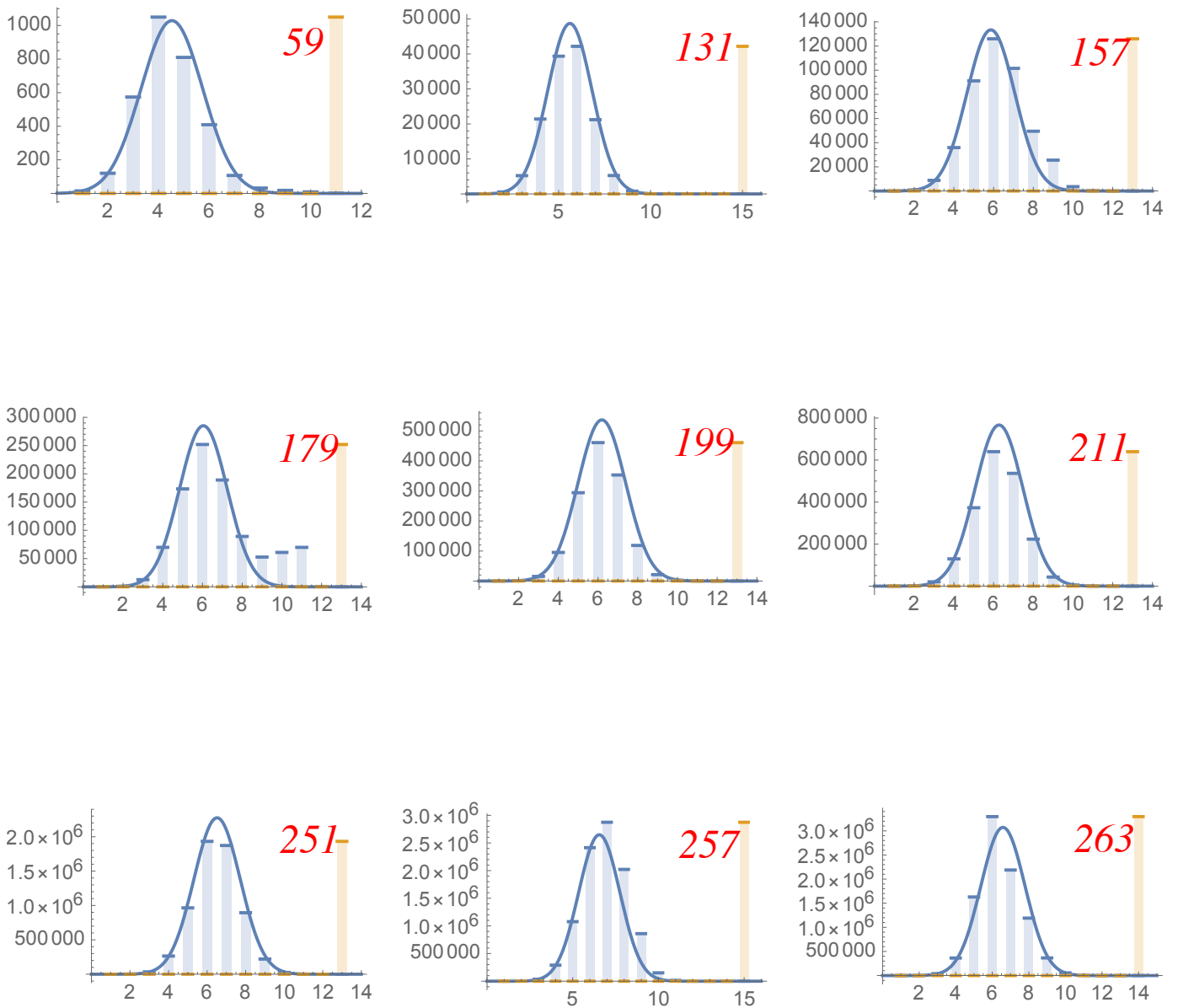


Figure 5: Primes with good gaussian approximation. Graphs of the functions $W(p, x)$ and $G(p, x)$ with x a continuous variable for the Gaussian.

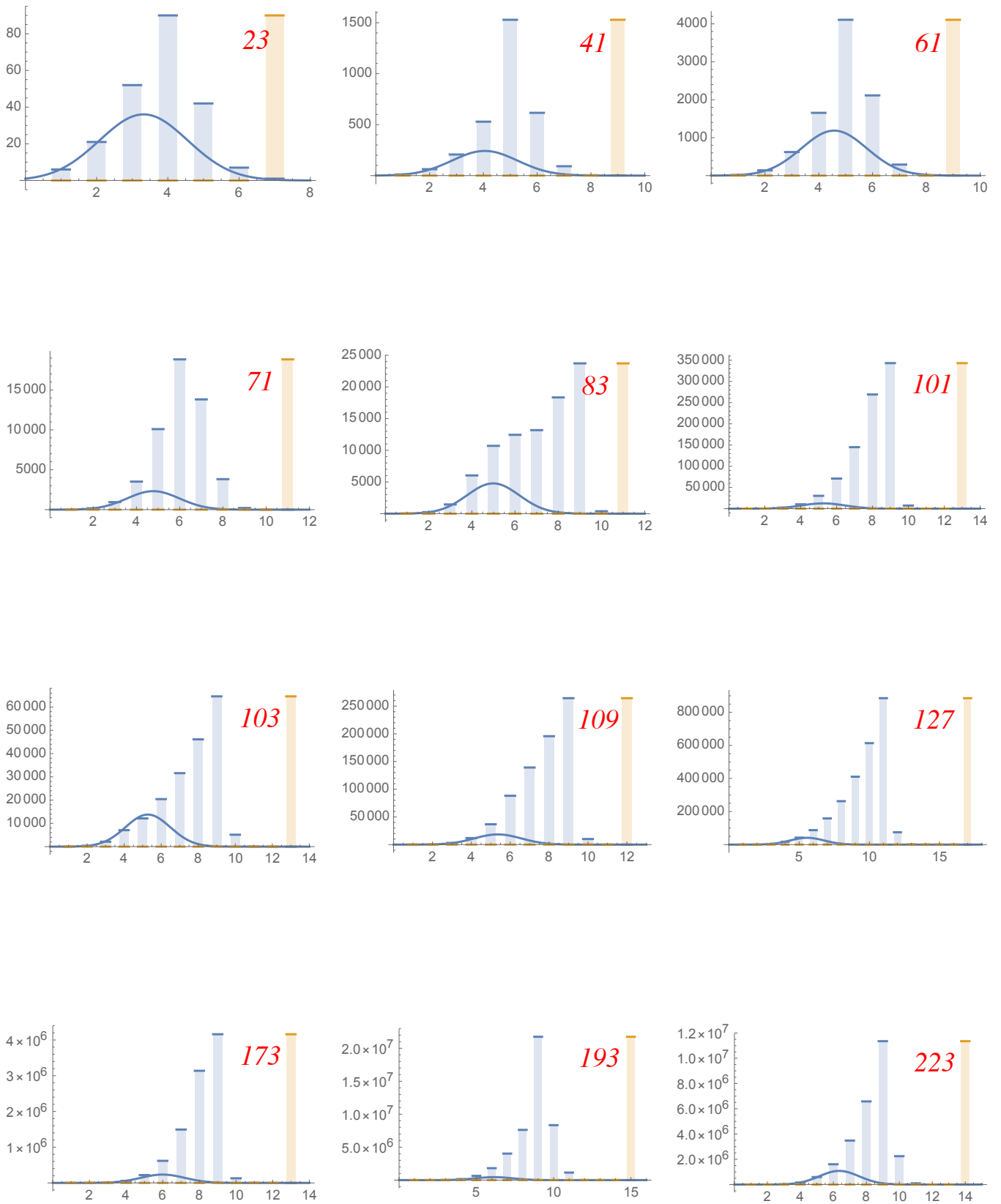


Figure 6: Primes with bad gaussian approximation.

References

- [1] L. Carlitz, *A theorem on permutations in a finite field*, Proc. Amer. Math. Soc. 11 (1960), 456–459. Errata ibid. 999–1000.
- [2] G.Jones, *Paley and the Paley graphs*, ArXiv 1702.00285
- [3] S. Graham, C. Ringrose *Lower bounds for least quadratic nonresidues*. Analytic number theory (Allerton Park, IL, 1989), 269–309, Progr. Math., 85, BirkhÄd’user Boston, Boston, MA, 1990.
- [4] H. L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Math., 227, Springer, Berlin, 1971.