COUNTING PLANES IN FINITE FIELDS

FRANÇOIS GUÉRITAUD

ABSTRACT. On the field with 2^n elements, we count the number of relationships of the form $a+b+c=0$, modulo the group generated by the Frobenius automorphism and multiplication by nonzero elements: there are roughly $\frac{2^n}{6n}$ relationships, meaning the group acts "mostly" freely on them. We also solve a similar counting problem on any finite field.

Keywords : finite upper half planes

CNRS – UMR 8524
Laboratoire Paul-Painlevé, université de Lille 1
59655 Villeneuve d'Ascq Cédex, France

Francois.Gueritaud@math.univ-lille1.fr

1. MOTIVATION : THE ADDITION TABLE IN $\mathbb{F}_{2^n}$.

Let ζ be a root of the irreducible polynomial X^6+X+1 on $\mathbb{F}_2$: the field with $2^6=64$ elements, $\mathbb{F}_{64}$, coincides with $\mathbb{F}_2[\zeta]$, and one can moreover show that ζ is primitive in $\mathbb{F}_{64}^\times$, i.e.

$$\mathbb{F}_{64}^\times = \{\zeta^{-31},\dots,1,\zeta,\dots,\zeta^{31}\} \simeq (\mathbb{Z}/63\mathbb{Z},+)$$

(just check that $\zeta^{63/3}$ and $\zeta^{63/7}$ are both different from 1).

Given $a,b\in[\![-31,31]\!]$ distinct, how do we find c such that $\zeta^a+\zeta^b=\zeta^c$? (This "discrete logarithm" problem is thought to be computationally hard.) It is enough to treat the case $b=0$, up to multiplying by ζ^b. Discarding $a=0$, this leaves $2^6-2=62$ relationships to determine. For example, we already know that

$$1+\zeta=\zeta^6 \; .$$

One easily checks the following relationships:

$$\begin{array}{rcl} 1+\zeta^{-11} &=& \zeta^{14} \\ 1+\zeta^{9} &=& \zeta^{-18} \\ 1+\zeta^{21} &=& \zeta^{-21}\; . \end{array}$$

By applying the Frobenius automorphism σ (i.e. doubling all exponents), one finds more relationships. Multiplying by powers of ζ yields more still (e.g. the first one gives $1+\zeta^{-1}=\zeta^5$). In fact, the four relationships above are enough to determine all others in just this way. Indeed, if we write, next to each Frobenius iterate of a relationship, the values of a for which it lets us express $1+\zeta^a$, we find

	$1+\zeta=\zeta^6$	$\pm1,\pm6,\pm5$	$1+\zeta^{-11}=\zeta^{14}$	$\pm11,\pm14,\pm25$
	$1+\zeta^2=\zeta^{12}$	$\pm2,\pm12,\pm10$	$1+\zeta^{-22}=\zeta^{28}$	$\pm22,\pm28,\pm13$
	$1+\zeta^4=\zeta^{24}$	$\pm4,\pm24,\pm20$	$1+\zeta^{19}=\zeta^{-7}$	$\pm19,\pm7,\pm26$
$(\sigma\downarrow)$	$1+\zeta^8=\zeta^{-15}$	$\pm8,\pm15,\pm23$		
	$1+\zeta^{16}=\zeta^{-30}$	$\pm16,\pm30,\pm17$		
	$1+\zeta^{-31}=\zeta^{3}$	$\pm31,\pm3,\pm29$		
	$1+\zeta^{9}=\zeta^{-18}$	$\pm9,\pm18,\pm27$	$1+\zeta^{21}=\zeta^{-21}$	±21

(The last two relationships are sent to themselves by σ, up to some factor ζ^ν and a permutation of the terms. Every relationship is sent to itself by $\sigma^6=\mathrm{Id}_{\mathbb{F}_{64}}$, but sometimes also by σ^d for d some divisor of 6.) One can check that all numbers from ± 1 to ± 31 arise in the table.

If we replace $64 = 2^6$ with 2^n, how many relationships will it take to determine the full addition table of $\mathbb{F}_{2^n}$? How many of them have an orbit of length n (i.e. maximal) under σ? A triple of exponents $\{a, b, c\}$ such that $\zeta^a + \zeta^b + \zeta^c = 0$ is the same as a 2-plane (on $\mathbb{F}_2$) within $\mathbb{F}_{2^n}$: namely the plane $\{0, \zeta^a, \zeta^b, \zeta^c\}$. One is thus led to compute the number N of orbits of such 2-planes, under the action of $\mathbb{F}_{2^n}^\times \rtimes \mathrm{Frob}$, where $\mathrm{Frob} = \{1, \sigma, \ldots, \sigma^{n-1}\}$ denotes the Galois group. One finds the following values:

$n =$	2	3	4	5	**6**	7	8	9	10	11	12	13	...
$N =$	1	1	2	1	**4**	3	8	11	20	31	64	105	...

Proposition 1. *For all $n \geq 2$, the number $N(n)$ of orbits of relationships in $\mathbb{F}_{2^n}$ is*

$$N(n) = \frac{1}{6n} \sum_{d|n} \phi(d) \left[2^{\frac{n}{d}} \left(1 + \underset{\text{if } 2|d}{3} + \underset{\text{if } 3|d}{2} \right) + \underset{\text{if } 3\nmid d}{2(-1)^{\frac{n}{d}}} \right]$$

where $\nu | d$ (resp. $\nu \nmid d$) means that ν divides (resp. does not divide) d, and $\phi(d)$ is the number of integers comprime to d in $\{1, \ldots, d\}$ (Euler's totient function). A term such as "$\underset{\text{if } 2|d}{3}$" is by definition 3 if $2|d$ and 0 otherwise.

This proposition will follow from an analogous count of orbits of planes in any finite field.

Corollary 2. *For large n, one has $N \sim \frac{2^n}{6n}$ and only $o(N)$ Frobenius orbits have length $< n$.*

Proof. Since $n = ab$ entails $\min\{a, b\} \leq \sqrt{n}$, every integer n has at most $2\sqrt{n}$ divisors. Therefore, for any $\varepsilon > 0$,

$$\sum_{d|n} \phi(d) \cdot 2^{\frac{n}{d}} \leq 2^{\frac{n}{1}} + 2\sqrt{n} \cdot n \cdot 2^{\frac{n}{2}} \underset{n \to \infty}{=} 2^n + o\left(2^{n\left(\frac{1}{2} + \varepsilon\right)} \right) .$$

Thus, the term $d = 1$ dominates in the formula of Proposition 1; in fact, the left half (roughly) of the digits of $N(n)$ coincide with those of $\frac{2^n}{6n}$. The corollary follows (an orbit of length k yields up to $6k$ relationships of the form $1 + \zeta^a = \zeta^c$, by multiplication by ζ^ν and switching sides). In fact, for n prime ≥ 5 the formula yields $N(n) = \frac{2^n - 2}{6n}$ and all orbits have length exactly n. $\square$

2. The general problem

Let q be a prime power, and $n > 1$ an integer. On the field $\mathbb{F}_q$ we may construct a vector space $(\mathbb{F}_q)^n$ of dimension n, which contains exactly

$$\frac{(q^n - 1)(q^n - q)}{(q^2 - 1)(q^2 - q)}$$

2-planes, by a classical argument.

Now identify $(\mathbb{F}_q)^n$ with $\mathbb{F}_{q^n}$, the field with q^n elements. On this space (and its 2-planes), there is an action by the Frobenius automorphism (of order n) and the multiplicative group $\mathbb{F}_{q^n}^\times$ (of order $q^n - 1$). We shall count the number $N = N(q, n)$ of orbits of 2-planes under the action of the group

$$\mathbb{F}_{q^n}^\times \rtimes \mathrm{Frob}$$

generated by these two transformations: if σ is the Frobenius map $X \mapsto X^q$, the semidirect product structure is given by $(u, \sigma^k)(v, \sigma^l) = (u\sigma^k(v), \sigma^{k+l})$, and the action on $\mathbb{F}_{q^n}$ by $(u, \sigma^k)x = u\sigma^k(x)$.

Note for example that all 2-planes of the form $u\mathbb{F}_{q^2}$ (with $u \in \mathbb{F}_{q^n}^\times$ and n being even) belong to the same orbit, of cardinality $\frac{q^n-1}{q^2-1}$.

Theorem 3. *For all $n \geq 2$ one has:*

$$\begin{aligned} N(q,n) &= \frac{1+(-1)^n}{4} + \frac{1}{n}\sum_{d|n}\phi(d)\left(\frac{d\wedge(q-1)}{2}\,\frac{q^{\frac{n}{d}}-1}{q-1}\right. \\ &\qquad \left. + \frac{d\wedge(q+1)}{2}\,\frac{q^{\frac{n}{d}}-(-1)^{\frac{n}{d}}}{q+1} - \underset{\text{if } d\wedge q=1}{q^{\frac{n}{d}-1}}\right) \end{aligned}$$

where $d \wedge \nu$ denotes the largest common divisor of d and ν.

The rest of this note is devoted to proving this theorem (and its special case Proposition 1). For this, consider not the 2-planes, but the *2-planes endowed with a basis seen up to homothety.* (A homothety is a multiplication by an element of $\mathbb{F}_q^\times$; note that multiplication by $u \in \mathbb{F}_{q^n}^\times$ is generally *not* a homothety in this sense). The group $\mathrm{PGL}_2(\mathbb{F}_q)$ acts simply transitively on such projectivized bases and it will be enough to quotient out by this action. Thus, one has

$$N = \left| \frac{\left\{\overline{(x,y)} \in (\mathbb{F}_{q^n}^\times)^2/\mathbb{F}_q^\times \mid \frac{x}{y} \notin \mathbb{F}_q\right\}}{(\mathbb{F}_{q^n}^\times/\mathbb{F}_q^\times \rtimes \mathrm{Frob}) \times \mathrm{PGL}_2(\mathbb{F}_q)} \right| .$$

Here the action is given by

$$\left(\mathbb{F}_q^\times u, \sigma^k, \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)\right)\cdot \mathbb{F}_q^\times \begin{pmatrix} x \\ y \end{pmatrix} = \mathbb{F}_q^\times \begin{pmatrix} u\sigma^k(\alpha x+\beta y) \\ u\sigma^k(\gamma x+\delta y)\end{pmatrix}$$

and it is a routine exercise to check that it is well-defined.

An element $g = \left(\mathbb{F}_q^\times u, \sigma^k, \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)\right)$ will sometimes be written $g = ([u], k, \varphi)$ for conciseness. There are $\frac{q^n-1}{q-1}n\frac{(q^2-1)(q^2-q)}{q-1} = nq(q+1)(q^n-1)$ possible values for g.

Fix $\overline{\left(\begin{smallmatrix}x\\ y\end{smallmatrix}\right)} \in (\mathbb{F}_{q^n}^\times)^2/\mathbb{F}_q^\times$, and define $\xi := \frac{x}{y} \in \mathbb{F}_{q^n} \smallsetminus \mathbb{F}_q$. Consider the fixed-point equation in $g = ([u], k, \varphi)$:

$$\mathbb{F}_q^\times \begin{pmatrix} x \\ y \end{pmatrix} = \mathbb{F}_q^\times \begin{pmatrix} u\sigma^k(\alpha x+\beta y) \\ u\sigma^k(\gamma x+\delta y)\end{pmatrix} .$$

For given k, φ, there exists at most one solution $u \in \mathbb{F}_{q^n}^\times/\mathbb{F}_q^\times$ (namely the value $u = \mathbb{F}_q^\times \frac{x}{\sigma^k(\alpha x+\beta y)}$), and it does exist if and only if

$$\frac{x}{y} = \frac{\sigma^k(\alpha x+\beta y)}{\sigma^k(\gamma x+\delta y)}$$

or equivalently

$$\xi = \sigma^k(\varphi(\xi))$$

where $\mathrm{PGL}_2(\mathbb{F}_q) \ni \varphi$ acts on $\mathbb{P}^1\mathbb{F}_{q^n}$ by Möbius transformations in the usual sense (e.g. of [finite] upper half planes) — one agrees that σ fixes infinity, and that $\mathbb{P}^1\mathbb{F}_{q^d} \subset \mathbb{P}^1\mathbb{F}_{q^n}$ when $d|n$. Only $\xi = \frac{x}{y}$ matters: y may be chosen at will inside $\mathbb{F}_{q^n}^\times$, which corresponds to "multiplication by ζ^a" in the Introduction.

Therefore, $N+1$ is just the number of orbits of $\mathbb{P}^1\mathbb{F}_{q^n}$ under the group $\mathrm{Frob} \times \mathrm{PGL}_2(\mathbb{F}_q)$, of order $n(q^3-q)$ (the extra "+1" corresponds to the orbit $\mathbb{P}^1\mathbb{F}_q$, which must be discarded since we request $\xi \notin \mathbb{F}_q$). Apply the class equation: the number of orbits is the average number of fixed points, i.e.

$$\begin{aligned} N+1 &= \frac{1}{n(q^3-q)}\sum_{k=0}^{n-1} N_k \\ \text{where } N_k &= \#\left\{(\varphi,\xi) \in \mathrm{PGL}_2(\mathbb{F}_q)\times\mathbb{P}^1\mathbb{F}_{q^n} \mid \varphi(\xi) = \sigma^k(\xi)\right\} . \end{aligned}$$

Note that $\sigma^k(\xi) = \varphi(\xi)$ implies $\sigma^{k\nu}(\xi) = \varphi^\nu(\xi)$ for all $\nu \in \mathbb{Z}$, by a straightforward induction (the coefficients of $\varphi \in \mathrm{PGL}_2(\mathbb{F}_q)$ are fixed under σ). Since $\sigma^l(\xi)$ depends solely on the residue class of l modulo n, one sees that $\sigma^k(\xi)$ belongs to the orbit $\mathrm{PGL}_2(\mathbb{F}_q)\cdot\xi$ if and only if $\sigma^{k\wedge n}(\xi)$ does. If $\mathbb{1}_U$ denotes the characteristic function of a set U, then by writing

$$N_k = \sum_{\xi\in\mathbb{P}^1\mathbb{F}_{q^n}} |\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{F}_q)}(\xi)|\, \mathbb{1}_{\mathrm{PGL}_2(\mathbb{F}_q)\cdot\xi}(\sigma^k(\xi))$$

we see immediately that $N_k = N_{k\wedge n}$. But for every divisor d of n, the number of values of k in $\{0,1,\dots,n-1\}$ such that $k\wedge n = d$ is exactly $\phi(\frac{n}{d})$. Therefore,

$$N+1 = \frac{1}{n(q^3-q)}\sum_{d|n}\phi\left(\frac{n}{d}\right)\sum_{\varphi\in\mathrm{PGL}_2(\mathbb{F}_q)} \#\left\{\xi\in\times\mathbb{P}^1\mathbb{F}_{q^n}\mid \varphi(\xi)=\sigma^d(\xi)\right\}\ .$$

Suppose that the order of φ does not divide $\frac{n}{d}$, i.e. $\varphi^{\frac{n}{d}} \neq 1$: then the relationship $\varphi(\xi) = \sigma^d(\xi)$ implies $\varphi^{\frac{n}{d}}(\xi) = \sigma^n(\xi) = \xi$, i.e. $\xi \in \mathrm{Fix}\left(\varphi^{\frac{n}{d}}\right) = \mathrm{Fix}(\varphi)$. The solutions are exactly the $\xi \in \mathrm{Fix}(\varphi)\cap\mathrm{Fix}(\sigma^d)$ that belong to $\mathbb{P}^1\mathbb{F}_{q^n}$: there may be either 0 or 1 or 2 of them; we will discuss the various possibilities below.

Proposition 4. *Suppose, on the contrary, that $\varphi^{\frac{n}{d}} = 1$. Then the equation $\varphi(\xi) = \sigma^d(\xi)$, i.e.*

$$\xi^{q^d} = \frac{\alpha\xi+\beta}{\gamma\xi+\delta}\ ,$$

has precisely q^d+1 distinct solutions ξ in $\mathbb{P}^1\mathbb{F}_{q^n}$.

Proof. (Fix representatives $\alpha,\beta,\gamma,\delta\in\mathbb{F}_q$.) The point $\xi=\infty$ is a solution if and only if $\gamma = 0$. As to finite solutions, they are the distinct roots of the polynomial

$$P := (\gamma X+\delta)X^{q^d} - (\alpha X+\beta)$$

in $\mathbb{F}_{q^n}$. Let

$$\mathcal{A} := \mathbb{F}_q[X]\left[\frac{1}{X-\eta}\right]_{\eta\in\mathbb{F}_q}$$

be the ring of rational functions whose denominator is split over $\mathbb{F}_q$, and let $\mathcal{I}$ be the ideal of $\mathcal{A}$ generated by P (i.e. by $X^{q^d} - \frac{\alpha X+\beta}{\gamma X+\delta}$). Whenever $X^{q^{\nu d}} - \varphi^\nu(X)\in\mathcal{I}$ and $\varphi^\nu = \left(\begin{smallmatrix}\alpha'&\beta'\\ \gamma'&\delta'\end{smallmatrix}\right)$, the following elements all belong to $\mathcal{I}$:

$$\begin{array}{rcl}
(\gamma'X+\delta')X^{q^{\nu d}} & - & (\alpha'X+\beta') \\
(\gamma'X^{q^d}+\delta')X^{q^{(\nu+1)d}} & - & (\alpha'X^{q^d}+\beta') \\
\left(\gamma'\dfrac{\alpha X+\beta}{\gamma X+\delta}+\delta'\right)X^{q^{(\nu+1)d}} & - & \left(\alpha'\dfrac{\alpha X+\beta}{\gamma X+\delta}+\beta'\right) \\
(\gamma'(\alpha X+\beta)+\delta'(\gamma X+\delta))\,X^{q^{(\nu+1)d}} & - & (\alpha'(\alpha X+\beta)+\beta'(\gamma X+\delta)) \\
X^{q^{(\nu+1)d}} & - & \dfrac{\alpha'\left(\frac{\alpha X+\beta}{\gamma X+\delta}\right)+\beta'}{\gamma'\left(\frac{\alpha X+\beta}{\gamma X+\delta}\right)+\delta'} \\
X^{q^{(\nu+1)d}} & - & \varphi^{\nu+1}(X)\ .
\end{array}$$

Thus, by induction, $X^{q^n} \equiv \varphi^{\frac{n}{d}}(X) = X$ modulo $\mathcal{I}$, which means that $X^{q^d} - \frac{\alpha X+\beta}{\gamma X+\delta}$ divides $X^{q^n} - X$ (which has a simple zero at every point of $\mathbb{F}_{q^n}$) in $\mathcal{A}$. In other words, P has all its roots in $\mathbb{F}_{q^n}$, and they are all simple except possibly the ones belonging to $\mathbb{F}_q$.

Let ξ be a multiple root of P in $\mathbb{F}_q$: then $P(\xi) = P'(\xi) = 0$ and $\xi^q = \xi$ together yield

$$\begin{array}{rcl} (\gamma\xi + \delta)\xi - (\alpha\xi + \beta) & = & 0 \\ \gamma\xi - \alpha & = & 0 \end{array}$$

hence $\delta\xi - \beta = 0$ and finally

$$\begin{pmatrix} \gamma & \alpha \\ \delta & \beta \end{pmatrix} \begin{pmatrix} \xi \\ -1 \end{pmatrix} = 0$$

which is impossible since $\varphi = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ is invertible. Therefore, all roots of P are simple and belong to $\mathbb{F}_{q^n}$. There are $q^d + 1$ of them, or exceptionally q^d when $\gamma = 0$ (but in that case we already had the solution $\xi = 0$). The Proposition is proved. $\square$

Observation 5. *The group* $\mathrm{PGL}_2(\mathbb{F}_q)$ *is a union of the following subgroups, which pairwise meet only at the identity:*

(1) Groups conjugated to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$, *of order* q, *numbering* $q+1$ *copies (characterized by their fixed slope), isomorphic to* $(\mathbb{F}_q, +)$. *Their nontrivial elements will be called* trigonalizable*; they fix exactly one point of* $\mathbb{P}^1\mathbb{F}_q$.

(2) Groups conjugated to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$, *of order* $q-1$, *numbering* $\frac{(q+1)q}{2}$ *copies (choice of two fixed slopes), isomorphic to* $\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. *Their nontrivial elements shall be called* diagonalizable*; they fix exactly two points of* $\mathbb{P}^1\mathbb{F}_q$.

(3) Groups stabilizing a pair of conjugate points $\eta, \overline{\eta}$ *of* $\mathbb{P}^1\mathbb{F}_{q^2} \smallsetminus \mathbb{P}^1\mathbb{F}_q$, *numbering* $\frac{q^2-q}{2}$ *copies (choice of the pair* $\{\eta, \overline{\eta}\}$*), isomorphic to* $\mathbb{Z}/(q+1)\mathbb{Z}$ *(being contained in the cyclic group* $\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{F}_{q^2})}(\eta, \overline{\eta}) \simeq \mathbb{F}_{q^2}^\times$ *and acting freely transitively on* $\mathbb{P}^1\mathbb{F}_q$*). Their nontrivial elements will be called* eigenvector-free *(in* $\mathbb{P}^1\mathbb{F}_q$*, that is).*

Indeed, each nontrivial element φ of $\mathrm{PGL}_2(\mathbb{F}_q)$ clearly belongs to a unique group from the list above, depending on where its fixed points lie in $\mathbb{P}^1\mathbb{F}_{q^2}$. Total cardinalities check out:

$$|\mathrm{PGL}_2(\mathbb{F}_q)| = q^3 - q = \underset{\text{identity}}{1} + \underset{\text{trigonalizable}}{(q-1)(q+1)} + \underset{\text{diagonalizable}}{(q-2)\frac{(q+1)q}{2}} + \underset{\text{e.v.-free}}{q\frac{q^2-q}{2}} \ .$$

(Note also the analogy with the classification of real Möbius transformations into parabolic, hyperbolic, and elliptic families according to the position of their fixed points in $\mathbb{P}^1\mathbb{C}$.) We may now write

$$\begin{aligned} N + 1 \quad = \quad & \frac{1}{n(q^3-q)} \times \sum_{d|n} \phi\left(\frac{n}{d}\right) \Bigg(\sum_{\substack{\varphi \in \mathrm{PGL}_2(\mathbb{F}_q) \\ \varphi^{\frac{n}{d}} = 1}} (q^d + 1) \\ & + \sum_{\substack{\varphi \in \mathrm{PGL}_2(\mathbb{F}_q) \\ \varphi^{\frac{n}{d}} \neq 1}} |\mathrm{Fix}(\varphi) \cap \mathrm{Fix}(\sigma^d) \cap \mathbb{P}^1\mathbb{F}_{q^n}| \Bigg) \ . \end{aligned}$$

Noticing that $\sum_{d|n} \phi(\frac{n}{d}) = n$ and $|\mathrm{PGL}_2(\mathbb{F}_q)| = q^3 - q$, and exchanging d with $\frac{n}{d}$, this amounts to

$$N = \frac{1}{n(q^3-q)} \sum_{d|n} \phi(d) \left(\sum_{\substack{\varphi \in \mathrm{PGL}_2(\mathbb{F}_q) \\ \varphi^d = 1}} q^{\frac{n}{d}} + \sum_{\substack{\varphi \in \mathrm{PGL}_2(\mathbb{F}_q) \\ \varphi^d \neq 1}} |\mathrm{Fix}(\varphi) \cap \mathrm{Fix}(\sigma^{\frac{n}{d}}) \cap \mathbb{P}^1\mathbb{F}_{q^n}| - 1 \right) .$$

For all $d \in \mathbb{N}$, the number of elements φ of $\mathrm{PGL}_2(\mathbb{F}_q)$ such that $\varphi^d = 1$ is

$$\begin{array}{rcll} A_d & = & 1 & \text{(the identity)} \\ & & +\frac{q(q+1)}{2} \cdot [d \wedge (q-1) - 1] & \text{(diagonalizables)} \\ & & +\frac{q(q-1)}{2} \cdot [d \wedge (q+1) - 1] & \text{(eigenvector-free)} \\ & & +(q+1) \cdot \underset{\text{if } d \wedge q \neq 1}{[q-1]} & \text{(trigonalizables)} \end{array}$$

or, rearranging the terms,

$$A_d = \frac{q(q+1)}{2}[d \wedge (q-1)] + \frac{q(q-1)}{2}[d \wedge (q+1)] - \underset{\text{if } d\wedge q = 1}{(q^2-1)} .$$

Among the $q^3 - q - A_d$ remaining elements φ, i.e. those satisfying $\varphi^d \neq 1$ (none of which is the identity!), the number $|\mathrm{Fix}(\varphi) \cap \mathrm{Fix}(\sigma^{\frac{n}{d}}) \cap \mathbb{P}^1\mathbb{F}_{q^n}| - 1$ will be 0 if φ is trigonalizable, 1 if φ is diagonalizable, and $(-1)^{\frac{n}{d}}$ if φ is eigenvector-free. Thus, using the shorthand $d_{q\pm 1}$ for $d \wedge (q \pm 1)$, we get

$$N = \frac{1}{n(q^3-q)} \sum_{d|n} \phi(d) \left(\begin{array}{l} \frac{q(q+1)}{2} \left[d_{q-1} q^{\frac{n}{d}} + (q - 1 - d_{q-1}) \right] \\ +\frac{q(q-1)}{2} \left[d_{q+1} q^{\frac{n}{d}} + (q + 1 - d_{q+1})(-1)^{\frac{n}{d}} \right] \\ -\underset{\text{if } d\wedge q=1}{(q^2-1)} \cdot q^{\frac{n}{d}} \end{array} \right) .$$

Observe finally that $\frac{q(q+1)}{2}(q-1) + \frac{q(q-1)}{2}(q+1)(-1)^{\frac{n}{d}}$ equals $q^3 - q$ if $\frac{n}{d}$ is even (i.e. $2d|n$) and 0 otherwise. The identity $\sum_{d|n} \phi(d) = n$ easily implies $\sum_{2d|n} \phi(d) = \frac{n}{2}$ if n is even and 0 otherwise, i.e. $\frac{1+(-1)^n}{4} n$ in general. It follows that

$$N = \frac{1+(-1)^n}{4} + \frac{1}{n(q^3-q)} \sum_{d|n} \phi(d) \left(\begin{array}{l} \frac{q(q+1)}{2}[d \wedge (q-1)](q^{\frac{n}{d}} - 1) \\ +\frac{q(q-1)}{2}[d \wedge (q+1)](q^{\frac{n}{d}} - (-1)^{\frac{n}{d}}) \\ -\underset{\text{if } d\wedge q=1}{(q^2-1)} \cdot q^{\frac{n}{d}} \end{array} \right) .$$

For instance, when d is coprime to the numbers $q-1, q, q+1$ (i.e. to $q^3 - q$), then the term in parentheses equals $q^{\frac{n}{d}} - q$ (if $\frac{n}{d}$ is odd) or $q^{\frac{n}{d}} - q^2$ (if $\frac{n}{d}$ is even). For d arbitrary, the term in parentheses will be at least as large as these values. The case $d = 1$ gives the leading term (as in Corollary 2) : $N \underset{n\to\infty}{\sim} \frac{q^n}{n(q^3-q)}$, meaning that there is only a very small proportion of fixed points in the class equation.

We may simplify some fractions for concision:

$$\begin{aligned} N &= \frac{1+(-1)^n}{4} + \sum_{d|n} \frac{\phi(d)}{n} \left(\frac{d\wedge(q-1)}{2} \frac{q^{\frac{n}{d}}-1}{q-1} + \frac{d\wedge(q+1)}{2} \frac{q^{\frac{n}{d}}-(-1)^{\frac{n}{d}}}{q+1} - \underset{\text{if } d\wedge q=1}{q^{\frac{n}{d}-1}} \right) \\ &= \frac{\mathbb{1}_{2\mathbb{N}}(n)}{2} + \sum_{d|n} \frac{\phi(d)}{2\frac{n}{d}} \left(\frac{q^{\frac{n}{d}} - 1}{d \vee (q-1)} - \underset{\text{if } d\wedge q=1}{\frac{2q^{\frac{n}{d}}}{d \cdot q}} + \frac{q^{\frac{n}{d}} - (-1)^{\frac{n}{d}}}{d \vee (q+1)} \right) \end{aligned}$$

(the first expression is that of Theorem 3). One easily recovers Proposition 1 by specializing to $q = 2$ and using again the identity $\sum_{2d|n} \phi(d) = \frac{n}{2} \mathbb{1}_{2\mathbb{N}}(n)$ encountered above.