THE QUASI-ORDER SPECTRUM OF ELEMENTS WITH PRIMITIVE NORM, AND THE EXACT RANGE OF VEGA'S CRITERION $b^2 \neq 2c$

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $\mathbb{F}_q$ be a finite field and let $f = X^2 + bX + c \in \mathbb{F}_q[X]$ be irreducible with c a primitive element of $\mathbb{F}_q$. Vega [1] proved that if $q+1 = 4\pi$ for an odd prime π, then f is a primitive polynomial if and only if $b^2 \neq 2c$, and asked whether the hypothesis $q + 1 = 4\pi$ is also necessary. It is not, and the exact list of fields over which the criterion is valid was determined shortly afterwards by Zhu and Wu [3]. We give a short treatment of that circle of results in which no polynomial is ever counted: everything about an element θ of a field with q^n elements whose norm generates $\mathbb{F}_q^\times$ is controlled by the single integer $g(\theta) = \gcd(\operatorname{ord}\theta,\, Q)$, $Q = (q^n-1)/(q-1)$, which for $n = 2$ is the quasi-order of the minimal polynomial of θ. Our new result is the exact spectrum of that invariant: the values realised by the elements outside $\mathbb{F}_q$ whose norm generates $\mathbb{F}_q^\times$ are exactly the integers $g \neq 1$ admitting a factorisation $Q = gm$ with $\gcd(m, q-1) = 1$, for every prime power q, every $n \geq 1$ and every g. Both directions come from a generator of the multiplicative group; the realisation half supplies, in complete generality, the existence statement that Zhu and Wu's Remark 7.4 says the proof of their Theorem 7.3 does not provide, and which they obtain instead by counting. The classification of the fields where Vega's criterion holds, a degree-n analogue of Vega's characterisation of the fields where every irreducible with primitive norm is primitive, and negative controls at $q = 3, 5, 13, 23$ all follow from divisor arithmetic. Every statement below is machine-checked in Lean 4 and is quantified over all q; no result rests on a finite case check.

1. Introduction

Let q be a prime power. Following Lidl and Niederreiter [5] — Definition 3.15 there, as cited by [1, Definition 1] — a polynomial $f \in \mathbb{F}_q[X]$ of degree $m \geq 1$ is *primitive* over $\mathbb{F}_q$ when it is the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^m}$, that is, of a generator of the cyclic group $\mathbb{F}_{q^m}^\times$. Deciding primitivity of a given irreducible polynomial normally means computing an order, so it is of interest to know when primitivity can instead be read off the coefficients.

For degree two the coefficients are two, and one of them is constrained for free: if $f = X^2 + bX + c$ is the minimal polynomial of $\theta \in \mathbb{F}_{q^2}$ then $c = \theta \cdot \theta^q = \mathrm{N}(\theta)$, and the norm of a generator of $\mathbb{F}_{q^2}^\times$ has order $(q^2-1)/(q+1) = q-1$, so c is then a primitive element of $\mathbb{F}_q$. The question is therefore what remains to be asked of b once c is primitive, and the answer depends on q. Vega's companion paper [2] proves that if $q+1$ is of one of the forms 2^t, π or 2π with π an odd prime, then every irreducible $X^2 + bX + c \in \mathbb{F}_q[X]$ with $b \neq 0$ and c primitive is already a primitive polynomial; [1] determines exactly which q have that property, and exhibits a second family of fields, disjoint from the first, where a single equation in the coefficients decides the question with no hypothesis on b at all. We quote that second statement verbatim from the e-print [1], where it is Theorem 7:

> Let q be a power of a prime number. If $q + 1 = 4\pi$, for some prime $\pi > 2$, then any irreducible polynomial of the form $f(x) = x^2 + bx + c \in \mathbb{F}_q[x]$, where c a primitive element of $\mathbb{F}_q$, is a primitive polynomial iff $b^2 \neq 2c$. In addition, if $b^2 = 2c$ then $f(x)$ is an irreducible non-primitive polynomial such that $\mathrm{qord}(f(x)) = 4$ and $\mathrm{ord}(f(x)) = 4(q-1)$.

Here qord is the *quasi-order* of [1, Definition 3]: for f of positive degree with $f(0) \neq 0$, the least positive integer ρ such that x^ρ is congruent modulo $f(x)$ to some element of $\mathbb{F}_q^\times$. The same invariant is called the *binomial order* by Zhu and Wu [3]. The paper [1] closes with a paragraph of future work whose first sentence is, again verbatim:

> As future work, it would be interesting to determine whether the sufficient condition in Theorem 7 is also necessary.

What is settled, and by whom. That question has an answer, and the answer was published before the present work was begun. One month after [1], Zhu and Wu [3] classified the finite fields with the property that the criterion $b^2 \neq 2c$ decides primitivity; their Theorem 6.3 reads, verbatim:

> A finite field $\mathbb{F}_q$ has property $\mathcal{P}$ if and only if q satisfies one of the following conditions: (i) $q+1 = \pi$ for some odd prime π; (ii) $q+1 = 2^t$ for some integer $t \geq 3$; (iii) $q+1 = 4\pi$ for some odd prime π.

Their property $\mathcal{P}$ is [3, Definition 6.1], also verbatim: "We say that a finite field $\mathbb{F}_q$ has property $\mathcal{P}$ if for any $b \in \mathbb{F}_q$ and any primitive element $c \in \mathbb{F}_q$, $f_{b,c}$ is primitive $\iff$ $f_{b,c}$ is irreducible and $b^2 \neq 2c$", where $f_{b,c}(X) = X^2 + bX + c$. Since a primitive polynomial is irreducible, that is exactly the property named in Definition 4.1 below.

Case (i) forces q even and cases (ii), (iii) force q odd, so the three cases are disjoint and $q+1 = 4\pi$ is one branch of three: the condition of Vega's Theorem 7 is sufficient and not necessary. The later version [4] of the same work goes further and constructs, for every finite field and every primitive c, the unique monic squarefree polynomial whose roots are exactly the b for which $X^2 + bX + c$ is primitive. We do not claim any of this classification as new; Sections 4 and 5 below reprove it, from a different starting point, and the point of reproving it is the route rather than the conclusion.

Results. Write K for a field with q^n elements, $\mathbb{F}_q \subseteq K$ for its subfield of order q, and

$$Q \;=\; \frac{q^n - 1}{q - 1} \;=\; 1 + q + \cdots + q^{n-1},$$

so that $\theta^Q = \mathrm{N}_{K/\mathbb{F}_q}(\theta)$ for $\theta \in K$. Attach to each $\theta \in K^\times$ the integer

$$g(\theta) \;=\; \gcd\big(\operatorname{ord}\theta,\; Q\big),$$

which for $n = 2$ is exactly the quasi-order of the minimal polynomial of θ (Proposition 2.3). Under the single hypothesis that θ^Q generates $\mathbb{F}_q^\times$, every question asked above about θ becomes a question about $g(\theta)$: the element lies in $\mathbb{F}_q$ iff $g = 1$, it is a primitive element of K iff $g = Q$, and for $n = 2$ its minimal polynomial satisfies $b^2 = 2c$ iff $g = 4$ (Lemmas 2.2 and 2.4). What is then needed is a description of which values of g occur, and that is the new theorem of this paper.

- **The spectrum** (Theorem 3.2). For every prime power q, every $n \geq 1$ and every integer g: some $\theta \in K \setminus \mathbb{F}_q$ whose norm generates $\mathbb{F}_q^\times$ has $g(\theta) = g$ if and only if $g \neq 1$ and $Q = gm$ for some m coprime to $q - 1$. Both halves are proved from a generator of $K^\times$ alone.
- **Consequences.** Every $\theta \notin \mathbb{F}_q$ with primitive norm is a primitive element of K iff 1 and Q are the only divisors of Q coprime to $q-1$ (Theorem 3.3); Vega's criterion is valid over $\mathbb{F}_q$ iff q is odd with $q+1 = 2^t$, $t \geq 3$, or $q+1 = 4\pi$ with π an odd prime, or q is even with $q+1$ prime (Theorem 4.3); the criterion fails at $q = 3, 5, 13, 23$ (Proposition 5.1); and its exceptional set is genuinely nonempty at $q = 11$ and empty at $q = 7$ (Proposition 5.2), although $7 \equiv 11 \equiv 3 \pmod 4$.

It is the realisation half of Theorem 3.2 that the literature does not contain in this generality. Zhu and Wu obtain the inclusion half for $n = 2$ and $q + 1 = 2^m\pi$ inside their Theorem 7.3, and their Remark 7.4 says, verbatim (with the internal cross-references resolved to the numbering of [3]):

> The proof of Theorem [7.3] does not guarantee that there indeed exists an irreducible quadratic polynomial whose binomial order is 2^m or $2^m\pi$. This fact only follows from the enumerations of primitive and irreducible non-primitive quadratic polynomials given in Proposition [7.9].

Theorem 3.2 supplies that existence directly — for every q, every degree n and every admissible index — with no enumeration, no count of irreducible or primitive polynomials, no quadratic characters and no Lucas sequences. The inclusion half at $n = 2$ is not claimed as new: for $q + 1 = 2^m\pi$ it is

Theorem 7.3 of [3], and for arbitrary q it is Proposition 4.5 of [4]. What neither version states is the realisation half.

Section 2 sets up the index and its dictionary, Section 3 proves the spectrum, Section 4 deduces the classification, Section 5 records the negative and non-vacuity controls, Section 6 the numerical record, and Section 7 states exactly what has been machine-checked and what has not.

2. The index of an element with primitive norm

Throughout, $q \geq 2$ and $n \geq 1$ are integers, K is a field with q^n elements — so that q is a prime power — and $Q = (q^n - 1)/(q - 1)$, equivalently $(q - 1)Q = q^n - 1$. We write $\mathbb{F}_q = \{x \in K : x^q = x\}$ for the subfield of order q and $\operatorname{ord}\theta$ for the multiplicative order of $\theta \in K^\times$.

Definition 2.1. The *index* of $\theta \in K^\times$ is $g(\theta) = \gcd(\operatorname{ord}\theta,\, Q)$.

Our standing hypothesis on θ is

$$\text{(H)} \qquad \theta \neq 0, \qquad \theta^q \neq \theta, \qquad \operatorname{ord}\big(\theta^Q\big) = q - 1.$$

The third condition says that the norm θ^Q is a primitive element of $\mathbb{F}_q$: an element of $K^\times$ lies in $\mathbb{F}_q^\times$ exactly when it is killed by $q-1$, so an element of order $q-1$ lies in $\mathbb{F}_q^\times$ and generates it. The second says $\theta \notin \mathbb{F}_q$.

Lemma 2.2 (Dictionary)**.** *Let $\theta \in K^\times$ satisfy $\operatorname{ord}(\theta^Q) = q - 1$ and put $g = g(\theta)$. Then*

(1) $\operatorname{ord}\theta = (q - 1)\, g$;
(2) $\gcd\big(Q/g,\ q - 1\big) = 1$;
(3) $\theta^q = \theta$ *if and only if* $g = 1$;
(4) $\operatorname{ord}\theta = q^n - 1$ *if and only if* $g = Q$.

Proof. (a) $\operatorname{ord}(\theta^Q) = \operatorname{ord}\theta/\gcd(\operatorname{ord}\theta, Q) = \operatorname{ord}\theta/g$, and this equals $q-1$ by hypothesis. (b) Suppose a prime p divided both Q/g and $q-1$. Then pg divides Q, and pg divides $(q-1)g = \operatorname{ord}\theta$ by (a); hence pg divides $\gcd(\operatorname{ord}\theta, Q) = g$, which is impossible since $g > 0$ and $p \geq 2$. (c) For $\theta \neq 0$, $\theta^q = \theta$ is equivalent to $\theta^{q-1} = 1$, i.e. to $\operatorname{ord}\theta \mid q - 1$; by (a) that says $(q-1)g \mid q - 1$, i.e. $g = 1$. (d) By (a), $\operatorname{ord}\theta = q^n - 1 = (q-1)Q$ is equivalent to $(q-1)g = (q-1)Q$, i.e. to $g = Q$. □

Part (a) already contains the second sentence of Vega's Theorem 7: an element of index 4 has order $4(q-1)$.

We now record what the index means for $n = 2$, which is the case of quadratic polynomials. Let $n = 2$, so $Q = q + 1$, and for $\theta \in K$ put

$$b(\theta) = -(\theta + \theta^q), \qquad c(\theta) = \theta^{q+1}.$$

Expanding $(X - \theta)(X - \theta^q)$ gives the identity

$$(X - \theta)(X - \theta^q) \;=\; X^2 + b(\theta)X + c(\theta), \tag{1}$$

valid in $K[X]$ for every θ. If $\theta^q \neq \theta$ then $\theta \notin \mathbb{F}_q$, so θ has degree 2 over $\mathbb{F}_q$ and (1) exhibits its minimal polynomial: $b(\theta)$ and $c(\theta)$ are fixed by the Frobenius $x \mapsto x^q$, hence lie in $\mathbb{F}_q$, and $X^2 + b(\theta)X + c(\theta)$ is the irreducible quadratic of which θ is a root. Conversely every irreducible $X^2 + bX + c \in \mathbb{F}_q[X]$ arises this way from either of its two roots in K. Under this correspondence, hypothesis (H) says precisely that $X^2 + bX + c$ is irreducible with c a primitive element of $\mathbb{F}_q$, and $\operatorname{ord}\theta = q^2 - 1$ says precisely that $X^2 + bX + c$ is a primitive polynomial.

Proposition 2.3. *Let $n = 2$ and let θ satisfy* (H)*, with minimal polynomial $f = X^2 + bX + c$. Then* $\operatorname{qord}(f) = g(\theta)$.

Proof. Modulo f we may identify $\mathbb{F}_q[x]/(f)$ with $\mathbb{F}_q(\theta) = K$, the class of x going to θ. So x^ρ is congruent modulo f to an element of $\mathbb{F}_q^\times$ exactly when $\theta^\rho \in \mathbb{F}_q^\times$, i.e. when $\theta^{\rho(q-1)} = 1$, i.e. when $\operatorname{ord}\theta \mid \rho(q-1)$. By Lemma 2.2(a) this reads $(q-1)g \mid \rho(q-1)$, i.e. $g \mid \rho$. The least positive such ρ is g. □

Lemma 2.4. *Let $n = 2$ and let $\theta \in K^\times$ satisfy $\operatorname{ord}(\theta^Q) = q - 1$ and $g(\theta) \neq 1$. Then, in every characteristic,*

$$b(\theta)^2 = 2\,c(\theta) \quad \Longleftrightarrow \quad g(\theta) = 4.$$

Proof. A direct expansion gives $b^2 - 2c = \theta^2\big(1 + \theta^{2(q-1)}\big)$, so for $\theta \neq 0$ the equation $b^2 = 2c$ is equivalent to $\theta^{2(q-1)} = -1$. By Lemma 2.2(a), $\theta^{k(q-1)} = 1$ is equivalent to $g \mid k$. In odd characteristic, $-1 \neq 1$, so $\theta^{2(q-1)} = -1$ says $g \mid 4$ and $g \nmid 2$, i.e. $g = 4$. In characteristic two, $-1 = 1$, so the equation says $g \mid 2$; but g divides $Q = q + 1$, which is odd, so this forces $g = 1$, excluded by hypothesis. Both sides of the stated equivalence are therefore false in characteristic two, since g odd cannot be 4. □

3. The spectrum of the index

Definition 3.1. An integer g is *admissible* for (q, Q) if $Q = gm$ for some integer m with $\gcd(m, q-1) = 1$; equivalently, if $g \mid Q$ and $\gcd(Q/g,\, q - 1) = 1$.

Theorem 3.2 (The quasi-order spectrum)**.** *Let $q \geq 2$ and $n \geq 1$, let K be a field with q^n elements and let $Q = (q^n - 1)/(q - 1)$. For an integer g, the following are equivalent:*

1. *there is a $\theta \in K$ with $\theta \neq 0$, $\theta^q \neq \theta$, $\operatorname{ord}(\theta^Q) = q - 1$ and $\gcd(\operatorname{ord}\theta,\, Q) = g$;*
2. *g is admissible for (q, Q) and $g \neq 1$.*

For $n = 2$: the quasi-orders of the irreducible quadratics over $\mathbb{F}_q$ with primitive constant term are exactly the admissible $g \neq 1$ for $(q, q + 1)$.

Proof. (1) ⇒ (2) is Lemma 2.2: parts (a) and (b) give the factorisation $Q = g \cdot (Q/g)$ with Q/g coprime to $q - 1$, and part (c) gives $g \neq 1$ because $\theta^q \neq \theta$.

(2) ⇒ (1) is the half that requires a construction. Write $Q = gm$ with $\gcd(m, q - 1) = 1$; then m divides Q, hence divides $q^n - 1$. Let γ be a generator of the cyclic group $K^\times$ and put $\theta = \gamma^m$. Then

$$\operatorname{ord}\theta = \frac{q^n - 1}{\gcd(q^n - 1, m)} = \frac{q^n - 1}{m} = \frac{(q-1)Q}{m} = (q-1)g,$$

and therefore

$$\gcd(\operatorname{ord}\theta, Q) = \gcd\big((q-1)g,\ gm\big) = g \cdot \gcd(q - 1, m) = g,$$

the last step by coprimality. Consequently $\operatorname{ord}(\theta^Q) = \operatorname{ord}\theta / \gcd(\operatorname{ord}\theta, Q) = (q-1)g/g = q - 1$, and $\theta \neq 0$. Finally $g \neq 1$ gives $\theta^q \neq \theta$ by Lemma 2.2(c). □

Nothing in the proof is a case check: q, n and g are arbitrary throughout, and the only structural input is that $K^\times$ is cyclic. The last clause of the theorem uses Proposition 2.3 and the correspondence of (1) to translate from elements to polynomials, and is stated for $n = 2$ only for a reason: for composite n an element outside $\mathbb{F}_q$ may have degree a proper divisor of n over $\mathbb{F}_q$, so its index need not be the quasi-order of a degree-n polynomial. The index itself, and the theorem, are unaffected.

Theorem 3.3. *With q, n, K, Q as in Theorem 3.2, the following are equivalent:*

1. *every $\theta \in K$ with $\theta \neq 0$, $\theta^q \neq \theta$ and $\operatorname{ord}(\theta^Q) = q - 1$ satisfies $\operatorname{ord}\theta = q^n - 1$;*
2. *every divisor m of Q with $\gcd(m, q - 1) = 1$ and $m \neq Q$ equals 1.*

Proof. (1) ⇒ (2): let $m \mid Q$ with $\gcd(m, q - 1) = 1$ and $m \neq Q$, and put $g = Q/m$. Then g is admissible and $g \neq 1$ (else $m = Q$), so Theorem 3.2 produces a θ satisfying (H) with $g(\theta) = g$. By (1) and Lemma 2.2(d), $g = Q$, hence $m = 1$.

(2) ⇒ (1): let θ satisfy (H) and put $g = g(\theta)$, $m = Q/g$. By Lemma 2.2(b), $\gcd(m, q-1) = 1$; by (c), $g \neq 1$, so $m \neq Q$. Hypothesis (2) gives $m = 1$, i.e. $g = Q$, and Lemma 2.2(d) gives $\operatorname{ord}\theta = q^n - 1$. □

Remark 3.4. Specialising Theorem 3.3 to $n = 2$, where $Q = q + 1$, is one line of divisor arithmetic, which we carry out here rather than in the formal development. For q odd, $\gcd(q + 1, q - 1) = 2$, so the divisors of $q + 1$ coprime to $q - 1$ are exactly the odd ones, namely the divisors of the odd part D of $q + 1$; since $q + 1$ is even, $D \neq q + 1$, and condition (2) of the theorem says $D = 1$. For q even, $q + 1$ is odd and coprime to $q - 1$, so condition (2) says that $q + 1$ is prime. Hence: *every* irreducible

$X^2 + bX + c \in \mathbb{F}_q[X]$ with c primitive is a primitive polynomial if and only if $q+1 = 2^t$ or $q+1$ is prime. The corresponding statement of [1] is its Theorem 6, the main theorem of that paper, which says that every irreducible $x^2+bx+c \in \mathbb{F}_q[x]$ with $b \neq 0$ and c a primitive element of $\mathbb{F}_q$ is primitive if and only if $q+1$ is of one of the forms 2^t, π or 2π for a positive integer t and a prime $\pi > 2$. It carries the extra hypothesis $b \neq 0$ and its answer contains one further family, $q+1 = 2\pi$; the discrepancy is exactly the polynomials with $b = 0$, which have index 2 (see Remark 4.7). For $n \geq 3$ neither [1] nor [3, 4] states an analogue, and Theorem 3.3 is not offered here as new mathematics: it is two lines from Theorem 3.2.

4. Vega's criterion and the fields over which it is valid

For the rest of the paper $n = 2$ and $Q = q+1$.

Definition 4.1. *Vega's criterion is valid over* $\mathbb{F}_q$ if for every θ in a field K with q^2 elements satisfying (H) one has

$$\operatorname{ord}\theta = q^2 - 1 \quad \Longleftrightarrow \quad b(\theta)^2 \neq 2\,c(\theta).$$

By (1) and the discussion after it, this is exactly the assertion that every irreducible $X^2+bX+c \in \mathbb{F}_q[X]$ with c a primitive element of $\mathbb{F}_q$ is a primitive polynomial if and only if $b^2 \neq 2c$.

Proposition 4.2. *Vega's criterion is valid over* $\mathbb{F}_q$ *if and only if*

$$\text{for every admissible } g \neq 1 \text{ for } (q, q+1): \qquad g = q+1 \iff g \neq 4. \tag{2}$$

Proof. Combine Lemma 2.2(d) (primitivity is $g = q+1$), Lemma 2.4 ($b^2 = 2c$ is $g = 4$) and Theorem 3.2 (the indices occurring are exactly the admissible $g \neq 1$). The direction "validity $\Rightarrow$ (2)" is where the spectrum is indispensable: an admissible $g \neq 1$ must first be realised by an actual θ before the hypothesis can be applied to it. The converse direction uses only Lemma 2.2 and Lemma 2.4, applied to a given θ. □

Condition (2) is pure divisor arithmetic and can be solved outright.

Theorem 4.3 (Classification)**.** *Let $q \geq 2$. Vega's criterion is valid over $\mathbb{F}_q$ if and only if*

- *q is odd and either $q+1 = 2^t$ with $t \geq 3$, or $q+1 = 4\pi$ with π an odd prime; or*
- *q is even and $q+1$ is prime.*

Proof. By Proposition 4.2 it suffices to solve (2).

Suppose q is even. Then $q+1$ is odd and coprime to $q-1$, so every divisor of $q+1$ is admissible, and every admissible g is odd, so $g \neq 4$ automatically. Thus (2) says: every divisor $g \neq 1$ of $q+1$ equals $q+1$, i.e. $q+1$ is prime.

Suppose q is odd and write $q+1 = 2^t D$ with D odd; then $t \geq 1$. Since $\gcd(q+1, q-1) = 2$, an integer m dividing $q+1$ is coprime to $q-1$ iff it is odd, so the admissible g are exactly those of the form $g = 2^t e$ with $e \mid D$: indeed $q+1 = gm$ with m odd forces $2^t \mid g$. Under this parametrisation (2) becomes

$$\text{for every } e \mid D: \qquad e = D \iff 2^t e \neq 4,$$

the constraint $g \neq 1$ being automatic because $t \geq 1$. Now:

- $t = 1$: $2e = 4$ is impossible for odd e, so the condition reads "every divisor of D equals D", i.e. $D = 1$, i.e. $q = 1$. So the criterion fails for every odd q with $q \equiv 1 \pmod 4$.
- $t = 2$: $4e = 4$ iff $e = 1$, so the condition reads "$e = D \iff e \neq 1$ for every $e \mid D$", i.e. D is prime; as D is odd, $q+1 = 4\pi$ with π an odd prime.
- $t \geq 3$: $2^t e \geq 8 > 4$ always, so the condition reads "every divisor of D equals D", i.e. $D = 1$, i.e. $q+1 = 2^t$.

Uniqueness of the decomposition $q+1 = 2^t D$ makes the three cases mutually exclusive and matches them with the three shapes in the statement. □

Theorem 4.3 is Theorem 6.3 of [3] in a different arrangement: their case (i), $q+1$ an odd prime, is our even case, and their (ii) and (iii) are our two odd cases; their property $\mathcal{P}$ is Definition 4.1, as recorded in Section 1.

Theorem 4.4 (Vega's Theorem 7)**.** *Let $q \geq 2$ and suppose $q+1 = 4\pi$ for some prime $\pi \neq 2$. Then Vega's criterion is valid over $\mathbb{F}_q$. In particular it is valid over $\mathbb{F}_{27}$, the only non-prime entry of the table of* [1]*, since $27+1 = 4 \cdot 7$.*

Proof. Such a q is odd, and $q+1 = 4\pi$ with π odd is the case $t = 2$, $D = \pi$ of Theorem 4.3. □

Theorem 4.5 (The other two branches)**.** *Vega's criterion is valid over $\mathbb{F}_q$ in each of the following two cases, neither of which is of the form $q+1 = 4\pi$ with π an odd prime:*

(1) *$q+1 = 2^t$ with $t \geq 3$;*
(2) *q even and $q+1$ prime.*

Proof. Immediate from Theorem 4.3; in case (1), $q+1 = 2^t$ with $t \geq 3$ makes q odd. □

Theorem 4.6 (The condition $q+1 = 4\pi$ is not necessary)**.** *Vega's criterion is valid over $\mathbb{F}_7$, while $7+1 = 8$ is not of the form 4π with π a prime different from 2. Hence the answer to the question of* [1] *quoted in Section 1 is negative.*

Proof. $8 = 2^3$, so Theorem 4.5(1) applies with $t = 3$; and $8 = 4\pi$ forces $\pi = 2$. A field with 49 elements exists, so the statement is not vacuous. □

The smallest odd witness is $q = 7$; the even branch supplies the smaller witnesses $q = 2$ and $q = 4$, where $q+1 = 3$ and $q+1 = 5$ are prime.

As stated in Section 1, this answer was already available in the literature [3] when the present development was made; Theorem 4.6 records it with an explicit witness in an explicit field.

Remark 4.7. Vega's Theorem 7, unlike the results of [2], carries no hypothesis $b \neq 0$, and the index explains why. In odd characteristic the same computation as in Lemma 2.4, with 4 replaced by 2, shows that $b(\theta) = 0$ is equivalent to $\theta^{q-1} = -1$, i.e. to $g(\theta) = 2$; and $g = 2$ is admissible for $(q, q+1)$ only when $(q+1)/2$ is odd, that is when $t = 1$. So for $q+1 = 4\pi$ there is no irreducible $X^2 + c$ with c primitive at all, and the hypothesis $b \neq 0$ would be vacuous. For $q \equiv 1 \pmod 4$, by contrast, $t = 1$ and the index 2 does occur; the resulting polynomial $X^2 + c$ is irreducible, is not primitive, and satisfies $0^2 \neq 2c$. That single polynomial is what breaks the criterion in the case $t = 1$ of Theorem 4.3. This remark is a paper argument and is not part of the formal development.

Remark 4.8. In the even branch of Theorem 4.3, q is a power of 2, say $q = 2^k$ with $k \geq 1$, and $q+1 = 2^k + 1$ is prime exactly when $2^k + 1$ is a Fermat prime. So the known part of that branch is $q \in \{2, 4, 16, 256, 65536\}$, and whether it is finite is the Fermat-prime problem.

5. Controls

The following two propositions are the negative and non-vacuity controls of the development. They are not new results — each is an instance of Theorem 4.3 or of Theorem 3.2 — but they are what rules out a misquantified reading of the statements above.

Proposition 5.1 (Negative controls)**.** *Vega's criterion is* not *valid over $\mathbb{F}_q$ for $q = 5$, $q = 13$, $q = 23$, or $q = 3$.*

Proof. All four are instances of Theorem 4.3. For $q = 5$ and $q = 13$ one has $q+1 = 6 = 2 \cdot 3$ and $q+1 = 14 = 2 \cdot 7$, both with $t = 1$. For $q = 23$, $q+1 = 24 = 2^3 \cdot 3$ has $t = 3$ and $D = 3 \neq 1$. For $q = 3$, $q+1 = 4 = 2^2 \cdot 1$ has $t = 2$ and $D = 1$, which is not prime. □

The first three show that no hypothesis on q can simply be dropped: q odd is not enough ($q = 5, 13$), and neither is $8 \mid q+1$ ($q = 23$, the worked example of [3, Example 7.10]). The fourth shows that the hypothesis $\pi > 2$ of Vega's Theorem 7 cannot be relaxed to $\pi \geq 1$: at $q = 3$ we have $q+1 = 4 = 4 \cdot 1$ and the criterion fails.

Proposition 5.2 (Non-vacuity and the residue class)**.** *Let K be a field with q^2 elements.*

(1) *For every $q \geq 2$ there exists $\theta \in K$ satisfying* (H) *with* $\operatorname{ord}\theta = q^2 - 1$*; in particular the hypotheses of Definition 4.1 are never vacuous.*
(2) *For $q = 11$ there exists $\theta \in K$ satisfying* (H) *with $b(\theta)^2 = 2c(\theta)$ and* $\operatorname{ord}\theta \neq q^2 - 1$*: an irreducible non-primitive $X^2 + bX + c$ with c primitive and $b^2 = 2c$.*
(3) *For $q = 7$ no $\theta \in K$ satisfying* (H) *has $b(\theta)^2 = 2c(\theta)$.*

Proof. (1) Apply the construction of Theorem 3.2 with $g = q+1$, $m = 1$: a generator of $K^\times$ has index $q+1$, hence lies outside $\mathbb{F}_q$ and has primitive norm. (2) $11+1 = 12 = 4\cdot 3$, so $g = 4$ is admissible with cofactor $m = 3$ coprime to $q-1 = 10$; Theorem 3.2 gives a θ with $g(\theta) = 4$, which satisfies $b^2 = 2c$ by Lemma 2.4 and is not primitive by Lemma 2.2(d), since $4 \neq 12$. (3) $7+1 = 8$, so an admissible g has odd cofactor and hence is 8; in particular $g = 4$ does not occur, and Lemma 2.4 excludes $b^2 = 2c$. □

Parts (2) and (3) together are a control on the residue class: $7 \equiv 11 \equiv 3 \pmod 4$, yet the exceptional set $\{b^2 = 2c\}$ is nonempty over $\mathbb{F}_{11}$ and empty over $\mathbb{F}_7$, so no condition on q modulo 4 governs it. What does govern it is visible in the same proof:

Remark 5.3. By Lemma 2.4 and Theorem 3.2, the exceptional set

$$E_q = \big\{(b,c) \;:\; X^2 + bX + c \text{ irreducible},\ c \text{ primitive},\ b^2 = 2c\big\}$$

over $\mathbb{F}_q$ is nonempty if and only if 4 is an admissible index, i.e. if and only if $q+1 = 4D$ with D odd, i.e. if and only if $q \equiv 3 \pmod 8$. For even q it is always empty. This one-line consequence is not part of the formal development, which contains only the two instances $q = 7$ and $q = 11$ of Proposition 5.2.

6. Numerical record

The computations described in this section lie outside the formal development; none of the theorems above depends on them. They were run as a check on the statements, and on the printed values of [1].

Three independent implementations of the criterion were compared. The first works directly in a field with q^2 elements, realised as $\mathbb{F}_p[x]/(f)$ with $\deg f = 2m$, locating $\mathbb{F}_q$ inside it as $\{x : x^q = x\}$ and testing the biconditional of Definition 4.1 over every pair (b,c) with c primitive by computing the multiplicative order of a root; it was run for every prime power $q \leq 32$. The second uses no field arithmetic at all, but instead the dictionary of Section 2, testing the corresponding conditions on the discrete logarithm i of θ for $0 \leq i < q^2 - 1$; it was run for every prime power $q \leq 1000$. The third evaluates the closed form of Theorem 4.3 against the description of the admissible indices for every prime power $q \leq 200000$. The three agree on every overlap, with no mismatch, and the second and third agree on all 636 fields with $q \leq 200000$ over which the criterion holds.

Among prime powers $q \leq 1000$, Vega's criterion is valid over $\mathbb{F}_q$ exactly for

$$q \in \{2, 4, 7, 11, 16, 19, 27, 31, 43, 67, 127, 163, 211, 243, 256, 283, 331, 523, 547, 691, 787, 907\}.$$

The first five entries with $q + 1 = 4\pi$ are $11, 19, 27, 43, 67$, reproducing the table of [1] including its non-prime entry $q = 27$; the entries $2, 4, 16, 256$ are the Fermat-prime cases of Remark 4.8, the entries $7, 31, 127$ are the cases $q + 1 = 2^t$ with $t \geq 3$, and the remaining fifteen entries, $q = 243 = 3^5$ among them, have $q + 1 = 4\pi$. Restricted to primes, the set is $\{2\}$ together with the primes $4\pi - 1$ for π an odd prime and the Mersenne primes $2^t - 1 \geq 7$; searches of the OEIS for the initial segments of that sequence and of the prime-power sequence above returned no match.

The counting side was checked as well. The number of pairs (b,c) with $X^2 + bX + c$ irreducible over $\mathbb{F}_q$, c primitive and $b^2 = 2c$ was measured to be $0, 8, 0, 12, 0, 0, 24, 0, 40, 0, 108, 96, 184$ at $q = 7, 11, 13, 19, 23, 31, 43, 47, 67, 127, 163, 211, 283$ and 24 at $q = 27$; these are $2\varphi(q-1)$ for the $q \equiv 3 \pmod 8$ in the list and 0 otherwise, in agreement with Remark 5.3 and with Lemma 2.2(a). Finally, every printed value of [1] was recomputed: its table of the first five fields with $q+1 = 4\pi$; the primitive elements $2, 6, 7, 11$ of $\mathbb{F}_{13}$ and the three degree-two examples there; the factorisation of $x^{12} - 2$ over $\mathbb{F}_{11}$ into the six quadratics $x^2 \pm 2x + 2$, $x^2 \pm 4x + 2$, $x^2 \pm 5x + 2$, of which the first two have quasi-order

4 and order 40 as printed there, the other four — which [1] states to be primitive — coming out with quasi-order 12 and order 120; the eight irreducible non-primitive $x^2 + bx + c$ with c primitive over $\mathbb{F}_{11}$; the orders 840, 280, 168 of the three examples over $\mathbb{F}_{29}$; and the two counting formulas of its Proposition 5 for $q \leq 43$. All values agreed.

One agreement is worth recording because it looks at first like a conflict. Over $\mathbb{F}_5$ and $\mathbb{F}_{13}$ the two counts of [1, Proposition 5] coincide, yet the criterion fails over both. There is no contradiction: that proposition, like the results of [2], counts only the polynomials with $b \neq 0$, whereas the criterion of Theorem 7 quantifies over all irreducible $X^2 + bX + c$; and for $q \equiv 1 \pmod 4$ the single polynomial $X^2 + c$ of Remark 4.7 is what breaks it.

7. Verification

Every statement of Sections 2–5 whose proof is given above — Lemmas 2.2 and 2.4, Theorems 3.2, 3.3, 4.3, 4.4, 4.5 and 4.6, Proposition 4.2 and Propositions 5.1 and 5.2 — has been machine-checked in Lean 4 [6] against Mathlib [7]. The development is five files and is stated for an arbitrary finite field K with $\operatorname{card} K = q^n$, so that every theorem is quantified over all q, and the spectrum over all n as well; nothing in it is a finite case check, and no appeal to compiled evaluation (`native_decide` or any equivalent) occurs anywhere. The axiom closure of each of the headline declarations is the standard one — propositional extensionality, quotient soundness and the axiom of choice — and there is no `sorry`. Concrete instances are obtained by supplying a field: $\mathbb{F}_{49}$ and $\mathbb{F}_{729}$ are taken from Mathlib's Galois fields, giving Theorem 4.6 and the $\mathbb{F}_{27}$ clause of Theorem 4.4 unconditionally. Three things above are paper arguments and are deliberately not formalised, and the reader should treat them as such: the identification of the quasi-order of [1, Definition 3] with the index (Proposition 2.3); the passage between elements θ of K and their minimal polynomials, of which only the coefficient identity (1) is checked formally, the statements themselves being phrased in terms of θ, $\theta^q \neq \theta$ and $\operatorname{ord}(\theta^{q+1}) = q - 1$; and Remarks 3.4, 4.7, 4.8 and 5.3. The computations of Section 6 are outside the formal development altogether. Repository reference to be added at submission.

8. What remains

Three questions are left open by the above. First, degree $n > 2$: Theorem 3.3 holds for every n, but the analogue of the coefficient equation $b^2 = 2c$ — a single polynomial identity in the coefficients that decides primitivity of degree-n irreducibles with primitive norm — is not known for $n \geq 3$, and neither is the set of pairs (q, n) for which one exists. For $n = 2$ the corresponding object has been constructed by Zhu and Wu [4]. Second, the exceptional set for composite odd part: when q is odd and $q+1 = 2^t D$ with D odd and composite, the pairs (b, c) that are irreducible and non-primitive with c primitive are exactly those of index $2^t e$ with e a proper divisor of D. The index says which pairs these are, but not what polynomial equation in (b, c) cuts them out; that is the optimality question settled in [4], and nothing here bears on it. Third, the arithmetic of the classification itself: whether Theorem 4.3 has infinitely many instances is open in each odd branch, being the question of whether there are infinitely many prime powers q with $q + 1 = 4\pi$, π prime, respectively $q + 1$ a power of 2.

References

[1] G. Vega, *Necessary and sufficient conditions on the order of a finite field $\mathbb{F}_q$ for the easy identification of primitive polynomials of degree* 2, arXiv:2607.01542v1 [math.NT] (1 July 2026). This is the only version. Theorem 6, Theorem 7, Definition 1, Definition 3, Proposition 5 and Table I are cited above, with the numbers of the compiled e-print, whose theorem environments share one flat counter (the theorem quoted in Section 1 carries the misleading source label `teodiez`, but is the seventh and prints as Theorem 7).

[2] G. Vega, *A characterization and an explicit description of all primitive polynomials of degree two*, Finite Fields Appl. **109** (2026), article 102716; DOI 10.1016/j.ffa.2025.102716. Also available as arXiv:2409.17147v1 [math.GM] (2 September 2024), where the title carries the additional words "over finite fields". The volume and article number are those of the Crossref record for the DOI and of the bibliographies of [3, 4]; the bibliography of [1] prints the volume as 16.

[3] L. Zhu and H. Wu, *On binomial order and primitivity of irreducible quadratic polynomials over finite fields*, arXiv:2608.01327v1 [math.NT] (2 August 2026). Definition 6.1 (property $\mathcal{P}$), Theorem 6.3 (the classification), Theorem 7.3, Remark 7.4, Proposition 7.9 and Example 7.10 are cited above; the title and all numbers are those of the compiled v1 e-print.

[4] L. Zhu and H. Wu, *The Optimal Coefficients-Based Criterion for Primitive Quadratic Polynomials over Finite Fields*, arXiv:2608.01327v2 [math.NT] (30 August 2026). The revised version of [3]; it constructs the optimal determining polynomial for every finite field, and its Proposition 4.5 is cited above. Property $\mathcal{P}$, its classification, Remark 7.4 and Example 7.10 of [3] do not appear in v2, which is why those are cited from v1. The v2 source lists the authors in the order H. Wu and L. Zhu.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications **20**, Addison-Wesley, 1983; Cambridge University Press, 1984. This is the printing cited by [1], whose Definition 1 quotes its Definition 3.15 as the definition of a primitive polynomial. A second edition appeared in the same series (Cambridge University Press, 1996; DOI 10.1017/CBO9780511525926, and dated 1997 in the bibliographies of [3, 4]).

[6] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635; DOI 10.1007/978-3-030-79876-5_37.

[7] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, 367–381; DOI 10.1145/3372885.3373824.