Jack's Exercises

Jack Westbrook

November 5, 2025

Problem 1

Question

Suppose a is an integer where $\text{ord}_2(a) = 1$. Prove that there are no integer solutions to the equation $y^{2m} = x^{2n} + a$ for $n, m \geq 0$.

Answer

Proof. $2 \mid K$ with multiplicity 1 is equivalent to $K \equiv 2 \mod 4$. We recall that squares are either 0 or $1 \mod 4$, so $x^{2n}, y^{2m} \equiv 0$ or $1 \mod 4$. These two facts prove the result when looking at the equation mod 4. ■

Problem 2

Question

Prove that there are no integral points on the elliptic curve $y^2 = x^3 - 9$.

Answer

Proof. Suppose we have an integer solution pair (x, y). Notice that x cannot be even; if it were, then $x^3 \equiv 0 \mod 4$; on the other hand, $y^2 + 9 \equiv 1$ or $2 \mod 4$.

Now, we rewrite our equation as follows:

$$(x-2)((x+1)^2+3) = y^2 + 1.$$

Because x is odd, the term $(x+1)^2 + 3 \equiv 3 \mod 4$; as such, there exists some prime $p \equiv 3 \mod 4$ dividing $(x+1)^2 + 3$. Then we get

$$y^2 + 1 = x^3 - 8 \equiv 0 \mod p.$$

But of course, this is also impossible because -1 is a square mod $p \neq 2$ if and only if $p \equiv 1 \mod 4$. ■

Proof. Suppose we have an integral solution to $x^3 = y^2 + 9$. In $\mathbb{Z}[i]$, we would then have $x^3 = (y+3i)(y-3i)$. First, we will show that $1 = (y+3i, y-3i)$. Letting d be the gcd in $\mathbb{Z}[i]$, we have $d \mid y + 3i - (y - 3i) = 6i$. Now the only prime that lies over 2 in $\mathbb{Z}[i]$ is $1+i$, and as 3 is inert in $\mathbb{Q}(i)/\mathbb{Q}$, we get that, because we may modify d by units, $d = (1+i)^a 3^b$. If $b > 0$, then $3 \mid d$ implies that $0 \equiv y + 3i \equiv y \mod 3$. But then $x^3 = y^2 + 9 \equiv 0 \mod 9$ implies that $3 \mid x$ as well, so by replacing x by $x/3$ and y by $y/3$, we get solutions to the new equation $3x^3 = y^2 + 1$. But then

$$y^2 + 1 = 3x^3 \equiv 0 \mod 3$$

implies that -1 is a quadratic residue modulo 3, which is obviously false. Thus we have $d = (1+i)^a$. If $a > 0$, then

$$0 \equiv y + 3i \equiv y - 3 \mod 1 + i.$$

Then for some $\alpha, \beta \in \mathbb{Z}$, we have $y - 3 = (\alpha + \beta i)(1 + i) = \alpha - \beta + (\alpha + \beta)i$. This implies $-\beta = \alpha$, and then that $2\alpha = y - 3$, hence $y \equiv 1 \mod 2$. Looking at the equation $x^3 = y^2 + 9$, we then see that

$$x^3 = y^2 + 9 \equiv 0 \mod 2$$

implying that $x \equiv 0 \mod 2$. Therefore $x^3 \equiv 0 \mod 8$, but then

$$y^2 + 1 \equiv y^2 + 9 = x^3 \equiv 0 \mod 8$$

which is impossible as -1 is not a quadratic residue modulo 8. This proves that $d = 1$. Now that $y^2 + 9 = (y + 3i)(y - 3i)$ is a perfect cube, and the latter two factors are coprime, each factor must be a perfect cube. This assertion uses the fact that $\mathbb{Z}[i]$ is a UFD.

Thus, for some integers a, b and unit $u \in \mathbb{Z}[i]^*$, we have a solution to

$$u(a + bi)^3 = y + 3i.$$

It's easy to verify that the units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$ by looking at the norms of elements in $\mathbb{Z}[i]$ and recalling that an element of the ring of integers is a unit iff it has norm 1. Expanding the above equation, we have

$$y + 3i = u(a^3 - 3ab^2 + i(3a^2b - b^3)).$$

Given our classification of what u must be, we must either have a solution to

$$\pm(3a^2b - b^3) = 3$$

or

$$\pm(a^3 - 3ab^2) = 3.$$

Let's first show that there are no solutions to the first equation. If there were, we would have $b^3 \equiv 0 \mod 3$, and thus $3 \mid b$. But then $9 \mid 3a^2b - b^3$, so also $9 \mid 3$ which is absurd.

Now let's show there are not solutions to the latter equation. If there were then $3 \mid a$ by considering the equation modulo 3, but then $9 \mid a^3 - 3ab^2$ so $9 \mid 3$ as well, again absurd. ■

Problem 3

Question

Prove that there are no integral points on the elliptic curve $y^2 = x^3 - 62$.

Answer

Proof. First of all, we notice that a solution to the equation $y^2 = x^3 - 62$ if and only if there is a solution to the equation $y^2 + x^3 + 62 = 0$, by replacing x by $-x$. Thus it suffices to show there is no integer solution to the latter equation.

Supposing x, y are integers solving the equation, we can rule out x being even as follows: if x were even, then

$$y^2 - 2 = -(x^3 + 64) \equiv 0 \mod 8.$$

However, 2 is not a square mod 8.

Now we rewrite our equation as follows:

$$y^2 - 2 = -(x + 4)((x - 2)^2 + 12).$$

Because x is odd, $(x-2)^2 \equiv 1 \mod 8$, so $(x-2)^2 + 12 \equiv -3 \mod 8$. Then there exists some prime $p \equiv \pm 3 \mod 8$ dividing $(x-2)^2 + 12$ as the only solution to $ab \equiv \pm 3 \mod 8$ is $a \equiv \pm 1 \mod 8$ and $b \equiv \pm 3 \mod 8$. But then we get that

$$y^2 - 2 = (x+4)((x-2)^2 + 12) \equiv 0 \mod p$$

which is impossible because 2 is a square mod p if and only if $p \equiv \pm 1 \mod 8$. ■

Problem 4

Question

Prove there are no integer solutions to the equation

$$y^2 - 3 = x^{16} + 2x^{14} + 3x^{12} + 4x^{10} + 5 + 6x^2 + 7x^4 + 8x^6 + 9x^8.$$

Answer

Proof. We rewrite the equation as

$$y^2 - 3 = (x^8 + x^6 + x^4 + x^2 + 5)(x^8 + x^6 + x^4 + x^2 + 1).$$

Notice now that the quadratic residues in $\mathbb{Z}/12\mathbb{Z}$ are $0, 1, 4$ and 9; moreover, $x^4 = x^2$ for every $x \in \mathbb{Z}/12\mathbb{Z}$. Thus, supposing a solution pair exists,

$$y^2 - 3 \equiv (4x^2 + 5)(4x^2 + 1) \mod 12.$$

The right hand side is $5 \mod 12$ when $3 \mid x$, which is impossible as 8 is not a quadratic residue in $\mathbb{Z}/12\mathbb{Z}$. If $3 \nmid x$, $x^2 \equiv 1$ or $4 \mod 12$; in either case, $4x^2 + 1 \equiv 5 \mod 12$.

Because every prime greater than 2 must be congruent to either ± 1 or $\pm 5 \mod 12$, we conclude that there is some prime $p \equiv \pm 5 \mod 12$ dividing $4x^2 + 1$ (because $4x^2 + 1$ is odd and has a prime factorization), and thus also $y^2 - 3$. We then have

$$y^2 - 3 \equiv 0 \mod p$$

which is impossible because 3 is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p = 2$, $p = 3$, or $p \equiv \pm 1 \mod 12$. To prove this, we first easily notice that 3 is a quadratic residue modulo 2 and 3. For $p > 3$, we compute that by quadratic reciprocity, if $p \equiv 1 \mod 4$ we have $(\frac{3}{p}) = (\frac{p}{3})$, and if $p \equiv 3 \mod 4$, then $(\frac{3}{p}) = -(\frac{p}{3})$. It's also easy to see that

$$(\frac{p}{3}) = \begin{cases} 1, & \text{if } p \equiv 1 \mod 3 \\ -1, & \text{if } p \equiv 2 \mod 3. \end{cases}$$

Now we can easily see that $(\frac{3}{p}) = 1$ precisely when $p \equiv 1 \mod 4$ and $p \equiv 1 \mod 3$, or when $p \equiv 3 \mod 4$ and $p \equiv 2 \mod 3$, or equivalently when $p \equiv 1 \mod 12$ or $p \equiv 11 \mod 12$. ■

Problem 5

Question

Prove that there are no integer solutions to $2y^2 = 2x^4 + 3x^2 + 1$.

Answer

Proof. We first notice that a solution pair exists to our given equation if and only if a solution pair exists for the equation $y^2 = 16x^4 + 24x^2 + 8$. This is because if (x, y) satisfies our original equation, then $(x, 4y)$ satisfies the new equation as

$$(4y)^2 = 16y^2 = 8(2x^4 + 3x^2 + 1) = 16x^4 + 24x^2 + 8,$$

and conversely if (x, y) satisfies the new equation, then $y \equiv 0 \mod 4$ since $y^2 \equiv 0 \mod 8$, hence $\frac{y}{4} \in \mathbb{Z}$, and $(x, \frac{y}{4})$ is a solution pair to the original equation because

$$2(\frac{y}{4})^2 = \frac{1}{8}(16x^4 + 24x^2 + 8) = 2x^4 + 3x^2 + 1.$$

We will now consider the equation $y^2 = 16x^4 + 24x^2 + 8$, and rewrite $y^2 = 16x^4 + 24x^2 + 8$ as $y^2 - 3 = 16x^4 + 24x^2 + 5 = (4x^2 + 1)(4x^2 + 5)$. Notice now that the quadratic residues in $\mathbb{Z}/12\mathbb{Z}$ are $0, 1, 4$ and 9. The right hand side is $5 \mod 12$ when $3 \mid x$, which is impossible as 8 is not a quadratic residue in $\mathbb{Z}/12\mathbb{Z}$. If $3 \nmid x$, $x^2 \equiv 1$ or $4 \mod 12$; in either case, $4x^2 + 1 \equiv 5 \mod 12$.

Because every prime greater than 2 must be congruent to either ± 1 or $\pm 5 \mod 12$, we conclude that there is some prime $p \equiv \pm 5 \mod 12$ dividing $4x^2 + 1$ (because $4x^2 + 1$ is odd and has a prime factorization), and thus also $y^2 - 3$. We then have

$$y^2 - 3 \equiv 0 \mod p$$

which is impossible because 3 is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p = 2$, $p = 3$, or $p \equiv \pm 1 \mod 12$. To prove this, we first easily notice that 3 is a quadratic residue modulo 2 and 3. For $p > 3$, we compute that by quadratic reciprocity, if $p \equiv 1 \mod 4$ we have $(\frac{3}{p}) = (\frac{p}{3})$, and if $p \equiv 3 \mod 4$, then $(\frac{3}{p}) = -(\frac{p}{3})$. It's also easy to see that

$$(\frac{p}{3}) = \begin{cases} 1, & \text{if } p \equiv 1 \mod 3 \\ -1, & \text{if } p \equiv 2 \mod 3. \end{cases}$$

Now we can easily see that $(\frac{3}{p}) = 1$ precisely when $p \equiv 1 \mod 4$ and $p \equiv 1 \mod 3$, or when $p \equiv 3 \mod 4$ and $p \equiv 2 \mod 3$, or equivalently when $p \equiv 1 \mod 12$ or $p \equiv 11 \mod 12$. ■

Proof. Using the same rearrangement, we can prove that there are no integer solutions to $2y^2 = 2x^4 + 3x^2 + 1$ by only modular arithmetic. First, we notice that $x \equiv 1 \mod 2$ by taking the equation mod 2. Therefore $x^2 \equiv 1 \mod 4$, so we get $2y^2 \equiv 2 \mod 4$. This implies that $y \equiv 1 \mod 2$ as well. Considering our equation modulo 3, we have

$$2y^2 \equiv 2x^2 + 1 \mod 3.$$

Then $x \equiv \pm 1 \mod 3$, implying $y \equiv 0 \mod 3$. Now we consider our equation modulo 5. If $x \equiv 0 \mod 5$, then

$$2y^2 \equiv 1 \mod 5$$

and as $3 = 2^{-1} \mod 5$, we would have $y^2 \equiv 3 \mod 5$ is impossible. Thus $x \not\equiv 0 \mod 5$, hence $x^4 \equiv 1 \mod 5$ and then

$$2y^2 \equiv 3x^2 + 3 \mod 5.$$

Multiplying each side by 3, we have $y^2 \equiv -(x^2 + 1) \mod 5$. But as $x^2 \equiv \pm 1 \mod 5$, we notice there is no solution if $x^2 \equiv 1 \mod 5$, and thus $x^2 \equiv -1 \mod 5$. Thus $x \equiv \pm 2 \mod 5$ and $y \equiv 0 \mod 5$. Thus $y \equiv 15 \mod 30$ and x can only be congruent to one of $\pm 7, \pm 13 \mod 30$. However, we then check that $2x^4$ ■

Problem 6

Question

Show that there are no integer solutions to the equation $y^2 = 4x^4 + 9x^2 + 5$.

Answer

Proof. We rewrite $y^2 = 4x^4 + 9x^2 + 5$ as $y^2 - 3 = 4x^4 + 9x^2 + 2 = (4x^2 + 1)(x^2 + 2)$. Notice that the quadratic residues in $\mathbb{Z}/12\mathbb{Z}$ are $0, 1, 4$ and 9. The right hand side of the given equation is $2, 5$ or $6 \mod 12$ if $x^2 \not\equiv 4 \mod 12$, which is impossible as neither are quadratic residues. Thus $4x^2 + 1 \equiv 5 \mod 12$.

Because every prime greater than 2 is congruent to either ± 1 or $\pm 5 \mod 12$, we conclude that there is some prime $p \equiv \pm 5 \mod 12$ dividing $4x^2 + 1$ ($4x^2 + 1$ is odd and thus has prime divisors strictly greater than 2), hence also $y^2 - 3$. We then have

$$y^2 - 3 \equiv 0 \mod p$$

which is impossible because 3 is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p = 2$, $p = 3$, or $p \equiv \pm 1 \mod 12$. To prove this, we first easily notice that 3 is a quadratic residue modulo 2 and 3. For $p > 3$, we compute that by quadratic reciprocity, if $p \equiv 1 \mod 4$ we have $(\frac{3}{p}) = (\frac{p}{3})$, and if $p \equiv 3 \mod 4$, then $(\frac{3}{p}) = -(\frac{p}{3})$. It's also easy to see that

$$(\frac{p}{3}) = \begin{cases} 1, & \text{if } p \equiv 1 \mod 3 \\ -1, & \text{if } p \equiv 2 \mod 3. \end{cases}$$

Now we can easily see that $(\frac{3}{p}) = 1$ precisely when $p \equiv 1 \mod 4$ and $p \equiv 1 \mod 3$, or when $p \equiv 3 \mod 4$ and $p \equiv 2 \mod 3$, or equivalently when $p \equiv 1 \mod 12$ or $p \equiv 11 \mod 12$. ■

Problem 7

Question

Find the greatest positive integer n such that p is a fourth root of unity in $\mathbb{Z}/n\mathbb{Z}$ for every prime $p \geq 11$.

Answer

Proof. We claim $n = 240$ is the solution. First, we will show that $n = 240$ works by proving that for every $p \geq 11$, $p^4 - 1 \equiv 0 \mod 240$. Notice that $p^4 - 1 = (p^2 + 1)(p - 1)(p + 1)$, where for each prime $p > 2$, each factor is even. If $p \equiv 1 \mod 4$ we have $p - 1 \equiv 0 \mod 4$ and the other factors are even implies $p^4 - 1$ is equivalent to $0 \mod 16$, and if $p \equiv 3 \mod 4$ then $p + 1 \equiv 0 \mod 4$ and the other factors even imply the result is divisible by 16 as well. Separately, because $p > 3$ implies $p \not\equiv 0 \mod 3$, we have $p^2 \equiv 1 \mod 3$, so indeed $3 \mid p^4 - 1$. Lastly, since $x^4 \equiv 1 \mod 5$ for every integer x indivisible by 5, we automatically get $p^4 - 1 \equiv 0 \mod 5$ since $p > 5$. Now because $16, 3$, and 5 are pairwise coprime and $p^4 - 1$ is divisible by each of them, we see $p^4 - 1 \equiv 0 \mod 240$.

For the reverse direction, suppose $p^4 - 1$ is divisible by n for every $p \geq 11$. Let $n = \prod p_i^{\alpha_i}$ be its prime factorization. Then $p^4 - 1$ is divisible by n if and only if it is divisible by $p_i^{\alpha_i}$ for each i by the Chinese remainder theorem. We have then for any $p \geq 11$ and any i that

$$p_i^{\alpha_i} \mid p^4 - 1 = (p^2 + 1)(p - 1)(p + 1)$$

only if p_i divides at least one of $p^2+1, p-1$, or $p+1$ for each i. If any $p_i \geq 11$, then we let $p = p_i$ and arrive at a contradiction because p_i does not divide p_i^2+1 or $p_i - 1$ or $p_i + 1$. Thus $n = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}7^{\alpha_4}$. We have by assumption that $2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}7^{\alpha_4} \mid (11^2+1)(11-1)(11+1) = 122 \cdot 10 \cdot 12 = 2^4 \cdot 3 \cdot 5 \cdot 61$ so indeed the maximum values for α_1, α_2 and α_3 are 4, 1 and 1 respectively while α_4 must be 0. Then $n \leq 2^4 \cdot 3 \cdot 5 = 240$, giving the result. ■

Problem 8

Question

Show that the only integral points on the elliptic curve $y^2 = x^3 - 11$ are $(3, \pm 4)$ and $(15, \pm 58)$.

Proof. Suppose $x, y \in \mathbb{Z}$ are such that $y^2 = x^3 - 11$. First, we recall that $\mathbb{Z}[\omega] = \mathcal{O}_{\mathbb{Q}(\sqrt{-11})}$ has class number 1 where $\omega = \frac{1+\sqrt{-11}}{2}$, i.e., is a PID. Then in $\mathbb{Z}[\omega]$, we have

$$(y + \sqrt{-11})(y - \sqrt{-11}) = x^3.$$

For ease of notation, we let $z = y + \sqrt{-11}$, $d = \gcd(z, \bar{z})$, and $\alpha = z/d \in \mathbb{Z}[\omega]$. We observe that $d \mid z - \bar{z} = 2\sqrt{-11}$, and that

$$N(2) = 4$$

and

$$N(\sqrt{-11}) = 11$$

So $N(\sqrt{-11})$ prime implies $\sqrt{-11}$ is irreducible. To show 2 is irreducible, it suffices to show there is no element in $\mathbb{Z}[\omega]$ with norm 2. Indeed, for $\zeta = a + b\omega$, we compute

$$N(\zeta) = \zeta\bar{\zeta} = (a + b\omega)(a + b\bar{\omega}) = a^2 + ab + 3b^2$$

which cannot equal 2, because a solution would enforce

$$a^2 + ab + b^2 \equiv 0 \mod 2$$

which implies that $a \equiv b \equiv 0 \mod 2$. But then 4 divides the left hand side, while 4 does not divide 2 obviously.

Therefore $d = 1$ or 2 or $\sqrt{-11}$ or $2\sqrt{-11}$. This shows $\bar{d} = \pm d$. Therefore $\gcd(\alpha, \bar{\alpha}) = 1$ since $\bar{\alpha} = \bar{z}/\bar{d} = \pm\bar{z}/d$. Since

$$x^3 = z\bar{z} = d^2\alpha\bar{\alpha}$$

it follows that for any irreducible $\pi \in \mathbb{Z}[\omega]$,

$$2\nu_\pi(d) + \nu_\pi(\alpha) + \nu_\pi(\bar{\alpha}) \equiv 0 \mod 3$$

and also that at most one of $\nu_\pi(\alpha), \nu_\pi(\bar{\alpha})$ is nonzero.

If $d = 1$, then $\nu_\pi(d) = 0$ for all π implies $\nu_\pi(\alpha) \equiv 0 \mod 3$ for all π, hence

$$z = d\alpha = \alpha = \zeta^3$$

for some $\zeta \in \mathbb{Z}[\omega]$.

If $d = 2$, then

$$\nu_\pi(d) = \begin{cases} 1, & \text{if } \pi = 2 \\ 0, & \text{otherwise} \end{cases}$$

so

$$\nu_\pi(\alpha) + \nu_\pi(\bar{\alpha}) \equiv \begin{cases} 1, & \text{if } \pi = 2 \\ 0, & \text{otherwise} \end{cases} \mod 3.$$

However, $2 \mid \alpha$ iff $2 \mid \bar{\alpha}$, which forces $\nu_2(\alpha) = \nu_2(\bar{\alpha}) = 0$. This contradicts the above equation for $\pi = 2$, so $d \neq 2$.

If $d = \sqrt{-11}$ or $d = 2\sqrt{-11}$, a very similar proof yields a contradiction, so we conclude $d = 1$ and $z = \zeta^3$ for some $\zeta \in \mathbb{Z}[\omega]$. We have

$$2\sqrt{-11} = z - \bar{z} = \zeta^3 - \bar{\zeta}^3 = (\zeta - \bar{\zeta})(\zeta^2 + \zeta\bar{\zeta} + \bar{\zeta}^2).$$

Letting $\zeta = a + b\omega$ with $a, b \in \mathbb{Z}$, we compute

$$\begin{aligned}
&\zeta - \bar{\zeta} = b\sqrt{-11} \\
&\zeta^2 = a^2 - 3b^2 + (b^2 + 2ab)\omega \\
&\zeta\bar{\zeta} = a^2 + 3b^2 + ab \\
&\bar{\zeta}^2 = a^2 - 3b^2 + (b^2 + 2ab)\bar{\omega} \\
&\zeta^2 + \zeta\bar{\zeta} + \bar{\zeta}^2 = 3a^2 - 2b^2 + 3ab \\
&2\sqrt{-11} = b\sqrt{-11}(3a^2 + 3ab - 2b^2)
\end{aligned}$$

which by the unique factorization gives the integral equation

$$2 = b(3a^2 + 3ab - 2b^2)$$

which leaves four possibilities for b: ± 1 or ± 2. If $b = 2$, then

$$1 = 3a^2 + 6a - 8 \Rightarrow a^2 + 2a - 3 = 0 \Rightarrow a = -3 \text{ or } 1.$$

If $b = -2$, then

$$-1 = 3a^2 - 6a - 8 \Rightarrow 3a^2 - 6a - 7 = 0$$

has no integer solutions because we would get $0 = 3a^2 - 6a - 7 \equiv -7 \mod 3$ is impossible.

If $b = 1$, then

$$2 = 3a^2 + 3a - 2 \Rightarrow 3a^2 + 3a - 4 = 0$$

also has no integer solutions since we would get $-4 \equiv 0 \mod 3$.

Lastly, if $b = -1$, then

$$-2 = 3a^2 - 3a - 2 \Rightarrow a(a-1) = 0 \Rightarrow a = 0 \text{ or } 1.$$

Thus the only possible values of ζ are

$$\zeta = 1 + 2\omega \text{ or } -3 + 2\omega \text{ or } -\omega \text{ or } 1 - \omega.$$

Then

$$y + \sqrt{-11} = z = \zeta^3 = -58 + \sqrt{-11} \text{ or } 58 + \sqrt{-11} \text{ or } 4 + \sqrt{-11} \text{ or } -4 + \sqrt{-11}.$$

Thus $y = \pm 4, \pm 58$ are the only possible values, and correspondingly we get $x = 3, 15$. ■

Problem 9

Question

Show that $f(X) = X^6 - 108 \in \mathbb{Q}[X]$ is irreducible.

Proof. By Gauss' Lemma, this polynomial is irreducible over $\mathbb{Q}$ iff it's irreducible over $\mathbb{Z}$, since it's primitive. Thus it suffices to show its irreducible over $\mathbb{F}_p$ for some prime p, since factorization over $\mathbb{Z}$ gives factorization in $\mathbb{F}_p$. For $p = 7$, we get $\bar{f}(X) = X^6 - 3 \in \mathbb{F}_7[X]$. We recall that $\mathbb{F}_q^\times$ is cyclic for every prime power q. Thus $\bar{f}$ has no roots in $\mathbb{F}_7$ since $x^6 = 1$ for all $x \in {\mathbb{F}_7}^\times$. If $\bar{f}$ had a quadratic factor in $\mathbb{F}_7$, then by modding out this quadratic factor from $\mathbb{F}_7[X]$, we would get a root of $\bar{f}$ in $\mathbb{F}_{7^2}$. Thus let $x \in \mathbb{F}_{7^2}^\times$ be such that $x^6 = 3$. But since $\mathbb{F}_{7^2}^\times$ is cyclic of order 48, it follows that the sixth powers form a subgroup of order 8, so then $1 = 3^8 = 3^2 = 2$, a contradiction.

Then the only remaining possibility is that $\bar{f}$ has a cubic factor. As before, this implies that $\bar{f}$ has a root in $\mathbb{F}_{7^3}^\times$. Since $\mathbb{F}_{7^3}^\times$ is cyclic of order 342, the sixth powers form a subgroup of order 57. But $3^{57} = (3^6)^9 \cdot 3^3 = 1^9 \cdot 27 = 3$ which again is a contradiction. ■