Diophantine sets of Fibonacci numbers

Florian Luca

June 8, 2017

Diophantine m-tuples

Let R be a commutative ring with 1. In general, $R = \mathbb{Z}$ although there are results when $R = \mathbb{Q}$, or $R = \mathbb{Z}[X]$, etc. For us, we will always work with $R = \mathbb{Z}$.

Definition

A Diophantine m-tuple in R is a set of m non-zero elements $\{a_1, \ldots, a_m\}$ of R such that $a_i a_j + 1 = \square$ in R for $1 \le i < j \le m$.

Example

Diophantus Found the example (over $\mathbb{Q}$) with $m = 4$:

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{68}{16}, \frac{105}{16}\right\}.$$

Example

Fermat Found the first example with $m = 4$ over $\mathbb{Z}$, namely:

$$\{1,\ 3,\ 8,\ 120\}.$$

What is of interest?

Given R, what is usually of interest is the size of m, the maximal length of a Diophantine m-tuple.

Take $m = 4$. Then there are infinitely Diophantine quadruples.

Example

The sets

$$\{k-1,\ k+1,\ 4k,\ 16k^3-4k\}$$

are Diophantine quadruples for all $k \geq 2$.

Example

The sets

$$\{F_{2n},\ F_{2n+2},\ F_{2n+4},\ 4F_{2n+1}F_{2n+2}F_{2n+3}\}$$

are Diophantine quadruples for all $n \geq 1$, where $F_0 = 0,\ F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$ is the Fibonacci sequence.

Example

One starts with a Diophantine triple $\{a, b, c\}$ and tries to extend it to a Diophantine m-tuple for $m \geq 4$. Usually, this involves the theory of Pell equations.

Take, for example, $\{a,\ b,\ c\} = \{1, 3, 8\}$. This corresponds to the case $n = 1$ of the previous example.

Then finding d such that

$$d + 1 = x^2, \quad 3d + 1 = y^2, \quad 8d + 1 = z^2$$

is equivalent to solving the system of Pellian equations

$$\begin{cases} y^2 - 3x^2 & = & -2, \\ z^2 - 8x^2 & = & -7. \end{cases}$$

The only such d is 120. This was shown to be so by Baker, Davenport in **1969**.

Why is there always a fourth number?

Arkin, Hoggatt and Straus, **1979** noted that if $\{a, b, c\}$ is a Diophantine triple with

$$ab + 1 = r^2, \quad bc + 1 = s^2, \quad ac + 1 = t^2,$$

setting

$$d = a + b + c + 2abc + 2rst, \tag{1}$$

then d fulfills:

$$ad + 1 = (at + rs)^2, \quad bd + 1 = (bs + rt)^2, \quad cd + 1 = (cr + st)^2.$$

Diophantine quadruples $a < b < c < d$ where d is given by (1) in terms of a, b, c are called regular.

Conjecture

(1) **Weak Dioph. Quintuple Conjecture** *There is no Diophantine quintuple.*

(2) **Strong Dioph. Quadruple Conjecture** *All Diophantine quadruples are regular.*

Dujella's Work

Concerning the Weak Diophantine Quintuple Conjecture, Dujella proved a series of important results from **2000** to **2004**.

For example, he proved that $m \leq 5$ and in fact, $m \leq 4$ holds with finitely many exceptions.

Very recently, He, Togbé, Ziegler **2016** announced a proof that $m \leq 4$ thus finishing off the Weak Diophantine Quintuple Conjecture.

The Strong Diophantine Quadruple Conjecture remains open.

Concerning the Strong Diophantine Quadruple Conjecture, Dujella proved it to be true for various parametric families of quadruples. One of his results from **2000** is the following:

Theorem

If

$$\{a,\ b,\ c,\ d\} = \{F_{2n},\ F_{2n+2},\ F_{2n+4},\ d\},$$

is a Diophantine quadruple, then $d = 4F_{2n+1}F_{2n+2}F_{2n+3}$.

The above result confirmed a conjecture of Bergum and Hoggatt.

One may ask if $d = 4F_{2n+1}F_{2n+2}F_{2n+3}$ can ever be a Fibonacci number, since then we would get an example of a Diophantine quadruple of Fibonacci numbers. However, Jones proved in **1978** that

$$F_{6n+5} < d < F_{6n+6}$$

holds for all $n \geq 1$.

A conjecture and a partial result

In **2015**, in a joint paper with He, Togbé we proposed the following conjecture.

Conjecture

There is no Diophantine quadruple of Fibonacci numbers $\{F_a, F_b, F_c, F_d\}$.

Earlier this year, in joint work with Y. Fujita, we proved the following partial result in the direction of the above conjecture.

Theorem

There are at most finitely many Diophantine quadruples of Fibonacci numbers.

The proof is ineffective so in order to settle completely the above conjecture new ideas (rather than just a long computation) are needed.

Special Diophantine triples of Fibonacci numbers

As we have seen,

$$F_{2n}F_{2n+2} + 1 = \square \qquad \text{and} \qquad F_{2n}F_{2n+4} + 1 = \square$$

for all n. Nevertheless there are examples (a, b) with $b - a > 4$ such that $F_a F_b + 1 = \square$, like

$$F_1 \cdot F_6 + 1 = 3^2, \quad F_3 \cdot F_{12} + 1 = 17^2, \quad F_4 \cdot F_{19} + 1 = 112^2.$$

In **2015**, He, L., Togbé proved the following theorem about triples of Fibonacci numbers $\{F_a, F_b, F_c\}$ when $(a, b) = (2n, 2n + 2)$.

Theorem

If $\{F_{2n}, F_{2n+2}, F_k\}$ is a Diophantine triple, then $k \in \{2n + 4, 2n - 2\}$, except when $n = 2$, case in which we have the additional solution $k = 1$.

Note that the exception $k = 1$ in case $n = 2$ is not truly an exception but it appears merely due to the fact that $F_1 = F_2$.

We collect some known facts about Fibonacci numbers.

Let

$$(\alpha, \beta) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)$$

be the two roots of the characteristic equation of the Fibonacci sequence $x^2 - x - 1 = 0$. Then the Binet formula for F_n is

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for all} \quad n \geq 0. \tag{2}$$

The Fibonacci sequence has a Lucas companion $\{L_n\}_{n\geq 0}$ given by $L_0 = 2,\ L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$. Its Binet formula is

$$L_n = \alpha^n + \beta^n \quad \text{for all} \quad n \geq 0. \tag{3}$$

There are many formulas involving Fibonacci and Lucas numbers. One which is useful to us is

$$L_n^2 - 5F_n^2 = 4(-1)^n \quad \text{for all} \quad n \geq 0. \tag{4}$$

A theorem of Siegel

We next recall a result of Siegel concerning the finiteness of the number of solutions of a hyperelliptic equation.

Lemma

Let $\mathbb{K}$ be any number field and $\mathcal{O}_{\mathbb{K}}$ be the ring of its algebraic integers. Let $f(X) \in \mathbb{K}[X]$ be a non constant polynomial having at least 3 roots of odd multiplicity. Then the Diophantine equation

$$y^2 = f(x)$$

has only finitely many solutions (x, y) in $\mathcal{O}_{\mathbb{K}}$.

Facts about quadruples

We next need one more fact about Diophantine quadruples. The following result is due to Fujita, Miyazaki **2016**.

Lemma

Let $\{a, b, c, d\}$ be a Diophantine quadruple with $a < b < c < d$. If $c > 722b^4$, then the quadruple is regular.

Lemma

If k is a fixed nonzero integer, then the Diophantine equation $kF_n + 1 = x^2$ has only finitely many integer solutions (n, x).

Proof. Inserting $F_n = (x^2 - 1)/k$ into (4) and setting $y := L_n$, we get

$$y^2 = 5F_n^2 + 4(-1)^n = \frac{1}{k^2}\left(5x^4 - 10x^2 + (5 \pm 4k^2)\right).$$

Should the above equation have infinitely many integer solutions (x, y) it would follow, by Lemma 11 (we take $\mathbb{K} = \mathbb{Q}$), that one of the polynomials

$$f_{\pm,k}(X) = 5X^4 - 10X^2 + (5 \pm 4k^2)$$

has double roots. However, $f_{\pm,k}(X)' = 20X(X^2 - 1)$, so the only possible double roots of $f_{\pm,k}(X)$ are 0 or ± 1. Since $f_{\pm,k}(0) = 5 \pm 4k^2 \neq 0$ and $f_{\pm,k}(\pm 1) = \pm 4k^2 \neq 0$, it follows that $f_{\pm,k}(X)$ has in fact only simple roots, a contradiction.

A result of Nemes and Pethő **1986**

All polynomials $P(X)$ of degree larger than 1 such that the Diophantine equation $F_n = P(x)$ has infinitely many integer solutions (n, x) were classified by the authors mentioned above. In particular, we could have used this classification in the proof of the previous lemma. However, we preferred to give a direct proof of the lemma especially since our proof reduces to an immediate verification of the hypotheses from Siegel's theorem.

Another lemma

Lemma

Assume that k is a positive integer such that the Diophantine equation

$$F_nF_{n+k} + 1 = x^2 \tag{5}$$

has infinitely many integer solutions (n, x). Then $k = 2, 4$ and all solutions have n even.

Proof. Using (2) and (3), we get

$$F_nF_{n+k}+1 = \frac{1}{5}(\alpha^n-\beta^n)(\alpha^{n+k}-\beta^{n+k})+1 = \frac{1}{5}\left(L_{2n+k}-(-1)^nL_k+5\right).$$

Thus, if (n,x) satisfy (5), then $L_{2n+k} = 5x^2+((-1)^nL_k-5)$. Inserting this into (4) (with n replaced by $2n+k$) and setting $y := F_{2n+k}$, we get

$$\begin{aligned} 5y^2 &= L_{2n+k}^2-4(-1)^k \\ &= 25x^4+10((-1)^nL_k-5)x^2+((-1)^nL_k-5)^2-4(-1)^k. \end{aligned}$$

Assuming that there are infinitely many integer solutions (n,x) to equation (5), it follows, by Lemma 11 (again, we take $\mathbb{K}=\mathbb{Q}$), that for $\zeta,\eta\in\{\pm1\}$, one of the polynomials

$$g_{\zeta,\eta,k}(X) = 25X^4+10(\zeta L_k-5)X^2+(\zeta L_k-5)^2-4\eta$$

has double roots.

Now

$$g_{\zeta,\eta,k}(X)' = X(100X^2 + 20(\zeta L_k - 5))$$

so the only zeros of the derivative of $g_{\zeta,\eta,k}(X)$ are 0 and $\pm\sqrt{\zeta L_k - 5}/5$.
Now

$$g_{\zeta,\eta,k}(0) = (\zeta L_k - 5)^2 - 4\eta.$$

If this is zero, then $\eta = 1$, and $\zeta L_k - 5 = \pm 2$. We thus get $\zeta L_k = 3, 7$, showing that $\zeta = 1$ and $k \in \{2, 4\}$. Thus, $k \in \{2, 4\}$ and $(-1)^n = \zeta = 1$, so n is even.
The other situation gives

$$g_{\zeta,\eta,k}(\pm\sqrt{\zeta L_k - 5}/5) = -4\eta.$$

Hence, this situation does not lead to double roots of $g_{\zeta,\eta,k}(X)$.

Finally, when $k = 2,\ 4$ it is easy to see that if $F_n F_{n+k} + 1$ is a square then n is even. Indeed for n odd we have in fact

$$F_n F_{n+2} - 1 = F_{n+1}^2 \quad \text{and} \quad F_n F_{n+4} - 1 = F_{n+3}^2.$$

Hence, if also one of $F_n F_{n+2} + 1$ or $F_n F_{n+4} + 1$ is a square, we would get two squares whose difference is 2, which of course is impossible.

The proof of the main result

For a contradiction, we assume that there are infinitely many Diophantine quadruples of Fibonacci numbers. We denote a generic one by $\{F_a, F_b, F_c, F_d\}$ with $a < b < c < d$. Hence, $d \to \infty$ over such quadruples. Since

$$F_a F_d + 1 = \square$$

and $d \to \infty$, it follows, by Lemma 13, that $a \to \infty$. We next show that both $d - c \to \infty$ and $c - b \to \infty$.

Assume say that $c - b = O(1)$ holds for infinitely many quadruples. Then there exists a positive integer k such that $c = b + k$ holds infinitely often. By Lemma 14, it follows that $k \in \{2, 4\}$ and b is even. If $k = 2$, then by Lemma 10 applied several times, it follows that $(a, b, c, d) = (a, a + 2, a + 4, a + 6)$, which contradicts the results of Dujella and Jones. Thus, we must have $c = b + 4$.

Consider the following equations

$$F_aF_b + 1 = x^2 \quad \text{and} \quad F_aF_{b+4} + 1 = y^2$$

with some integers x and y. Multiplying the two relations above we get

$$F_a^2F_bF_{b+4} + F_a(F_b + F_{b+4}) + 1 = (xy)^2.$$

Since $F_bF_{b+4} = F_{b+2}^2 - 1$ and $F_{b+4} + F_b = 3F_{b+2}$, we get

$$(xy)^2 = F_a^2(F_{b+2}^2 - 1) + 3F_aF_{b+2} + 1 = \left(F_aF_{b+2} + \frac{3}{2}\right)^2 - \left(\frac{5}{4} + F_a^2\right),$$

so

$$\begin{aligned} 4F_a^2 + 5 &= (2F_aF_{b+2} + 3)^2 - (xy)^2 \\ &= (2F_aF_{b+2} + 3 - xy)(2F_aF_{b+2} + 3 + xy). \end{aligned}$$

The right–hand side is

$$\geq 2F_aF_b + 3 + xy \gg \alpha^{a+b},$$

while the left–hand side is $\ll \alpha^{2a}$. Thus $\alpha^{2a} \gg \alpha^{a+b}$, showing that $b - a = O(1)$.

By Lemma 14 again, it follows that $b - a \in \{2, 4\}$ with finitely many exceptions. The case $b = a + 2$ leads, via Lemma 10 applied again several times, to the situation $(a, b, c, d) = (a, a + 2, a + 4, a + 6)$, which we already saw that it is impossible, while the situation $b = a + 4$ together with $c = b + 4 = a + 8$, leads to

$$F_a F_{a+8} + 1 = \square,$$

which, by Lemma 14, can have only finitely many solutions a. Thus, $c - b \to \infty$. Notice that d was not used in the above argument (we only worked with the triple $\{F_a, F_b, F_c\}$). Thus, the same argument implies that $d - c \to \infty$ by working with the triple $\{F_b, F_c, F_d\}$ instead of the triple $\{F_a, F_b, F_c\}$.

Assume next that $c \geq 4b + 15$ infinitely often. Then

$$F_c \geq F_{4b+15} = F_{16}F_{4b} + F_{15}F_{4b-1} > 722F_{4b} > 722F_b^4,$$

so, by Lemma 12, it follows that the Diophantine quadruple $\{F_a, F_b, F_c, F_d\}$ is regular. Hence,

$$F_d = F_a+F_b+F_c+2F_aF_bF_c+2\sqrt{(F_aF_b + 1)(F_bF_c + 1)(F_aF_c + 1)}.$$

Since $F_m = \dfrac{\alpha^m}{\sqrt{5}}(1 + o(1))$ as $m \to \infty$, and $a \to \infty$, we get

$$\frac{\alpha^d}{\sqrt{5}}(1 + o(1)) = \frac{4}{5^{3/2}}\alpha^{a+b+c}(1 + o(1)),$$

showing that

$$\left|\alpha^{d-a-b-c} - \frac{4}{5}\right| = o(1), \quad \text{as} \quad a \to \infty.$$

Thus, $\alpha^{d-a-b-c} = 4/5$, which is impossible because $4/5$ does not belong to the multiplicative group generated by α.

Hence, $c \leq 4b + 14$ holds with finitely many exceptions. Thus, we arrived at the scenario where

$$F_b F_c + 1 = x^2$$

has infinitely many integer solutions (b, c, x) with $b < c \leq 4b + 14$. Now the Corvaja, Zannier method based on the Subspace Theorem (see also some of Fuchs early papers) leads to the conclusion that there exists a line parametrized as

$$b = r_1 n + s_1, \quad c = r_2 n + s_2$$

for positive integers $r_1,\ r_2$ and integers $s_1,\ s_2$, such that for infinitely many positive integers n, there exists an integer v_n such that

$$F_{r_1 n + s_1} F_{r_2 n + s_2} + 1 = v_n^2.$$

We sketch the details of this deduction at the end.

The condition $c \leq 4b + 14$ implies $r_2 \leq 4r_1$. The condition $c > b$ together with the fact that $c - b \to \infty$, implies that $r_2 > r_1$. By writing

$$s_1 = r_1 q + s_1' \quad \text{with} \quad q = \lfloor s_1/r_1 \rfloor \quad \text{and} \quad s_1' \in \{0, 1, \ldots, r_1 - 1\},$$

and making the linear shift

$$n \mapsto n + \lfloor s_1/r_1 \rfloor,$$

we may assume that $s_1 \in \{0, 1, \ldots, r_1 - 1\}$. Finally, we may assume that

$$\gcd(r_1, r_2) = 1$$

(otherwise, we let $\delta := \gcd(r_1, r_2)$ and replace n by δn).

We may also assume that both $r_1 n$ and $r_2 n$ are even infinitely often (this is the case when n is even, for example), so $\beta^{r_1 n} = \alpha^{-r_1 n}$ and $\beta^{r_2 n} = \alpha^{-r_2 n}$. The other cases can be dealt with by similar arguments.

We now use formula (2) and get

$$\begin{aligned} F_{r_1 n+s_1} F_{r_2 n+s_2} + 1 & = \frac{1}{5}(\alpha^{r_1 n+s_1} - \beta^{r_1 n+s_1})(\alpha^{r_2 n+s_2} - \beta^{r_2 n+s_2}) + 1 \\ & =: \frac{\alpha^{-n(r_1+r_2)}}{5} P_{r_1,r_2,s_1,s_2}(\alpha^n), \end{aligned}$$

where

$$P_{r_1,r_2,s_1,s_2}(X) = (\alpha^{s_1} X^{2r_1} - \beta^{s_1})(\alpha^{s_2} X^{2r_2} - \beta^{s_2}) + 5X^{r_1+r_2}.$$

Let $\mathbb{K} := \mathbb{Q}(\sqrt{5})$. We thus get that

$$P_{r_1,r_2,s_1,s_2}(\alpha^n) = \left(\frac{\alpha^{-n(r_1+r_2)/2}}{\sqrt{5}}\right)^2 v_n^2, \tag{6}$$

infinitely often with some integer v_n, and the right–hand side above is a square in $\mathcal{O}_{\mathbb{K}}$ for infinitely many n. Thus, the Diophantine equation

$$y^2 = P_{r_1,r_2,s_1,s_2}(x)$$

has infinitely many solutions (x, y) in $\mathcal{O}_{\mathbb{K}}$. In particular, $P_{r_1,r_2,s_1,s_2}(X)$ can have at most two roots of odd multiplicity by Lemma 11. In fact, we shall show that it has no root of odd multiplicity.

Indeed, assume that z_0 is some root of odd multiplicity of $P_{r_1,r_2,s_1,s_2}(X)$. Let D be any positive integer. Infinitely many of our n will be in the same residue class r modulo D. Thus, such n can be written under the form $n = Dm + r$. We may then replace X by $X^D\alpha^r$ and work with $Q(X) := P_{r_1,r_2,s_1,s_2}(X^D\alpha^r)$. Equation

$$y^2 = Q(x)$$

still has infinitely many solutions (x, y) in $\mathcal{O}_{\mathbb{K}}$ (just take in (6) positive exponents n which are congruent to r modulo D), yet $Q(X)$ has at least D roots of odd multiplicity, namely all the roots of $X^D\alpha^r - z_0$. Since D is arbitrary (in particular, it can be taken to be any integer larger than 2), we conclude that this is possible only when $P_{r_1,r_2,s_1,s_2}(X)$ has all its roots of even multiplicity, so it is associated to the square of a polynomial in $\mathcal{O}_{\mathbb{K}}[X]$.

So, let us write

$$P_{r_1,r_2,s_1,s_2}(X) = \gamma(X^{2r_1+2r_2} + \gamma_1 X^{2r_2} + \gamma_2 X^{r_1+r_2} + \gamma_3 X^{2r_1} + \gamma_4)$$

for some nonzero coefficients $\gamma, \gamma_1, \gamma_2, \gamma_3, \gamma_4$. Since $r_1 < r_2$, all the above monomials are distinct. Write $P_{r_1,r_2,s_1,s_2}(X) = \gamma R(X)^2$ for some monic polynomial $R(X) \in \mathbb{K}[X]$ and let us identify some monomials in $R(X)$. Certainly, $R(0) \neq 0$. Further, $\deg R(X) = r_1 + r_2$ and the last nonzero monomial in $R(X)$ is certainly X^{2r_1}. Hence, we get

$$P_{r_1,r_2,s_1,s_2}(X) = \gamma(X^{r_1+r_2} + \cdots + \delta_1 X^{2r_1} + \delta_0)^2,$$

for some nonzero coefficients $\delta_0, \ \delta_1$ which can be computed, up to sign, in terms of $\gamma, \ \gamma_3, \ \gamma_4$.

Assume first that $R(X)$ does not have other monomials. Then

$$\gamma R(X)^2 = \gamma(X^{2r_1+2r_2} + 2\delta_1 X^{3r_1+r_2} + \delta_1^2 X^{4r_1} + 2\delta_0 X^{r_1+r_2} + 2\delta_0\delta_1 X^{2r_1} + \delta_0^2).$$

The second leading monomial above is $X^{3r_1+r_2}$ and matching it with the second leading monomial in $P_{r_1,r_2,s_1,s_2}(X)$, which is X^{2r_2}, we get $r_2 = 3r_1$. Hence, since $\gcd(r_1, r_2) = 1$, we get $(r_1, r_2) = (1, 3)$.

Assume next that $R(X)$ contains monomials of intermediary degrees between $r_1 + r_2$ and $2r_1$. Let the leading one of them be of degree e. Thus,

$$R(X) = X^{r_1+r_2} + \delta X^e + \cdots + \delta_1 X^{2r_1} + \delta_0,$$

with some nonzero coefficient δ. Then the second leading monomial of $\gamma R(X)^2$ is $X^{r_1+r_2+e}$ and matching that with the second leading monomial appearing in $P_{r_1,r_2,s_1,s_2}(X)$ which is X^{2r_2}, we get that $r_1 + r_2 + e = 2r_2$, therefore $e = r_2 - r_1$. The condition $e > 2r_1$ yields $r_2 > 3r_1$. Now let us look at X^{2e}. It might appear with nonzero coefficient in $R(X)^2$, or not. If it does, its degree must match the degree of one of the monomials of a lower degree in $P_{r_1,r_2,s_1,s_2}(X)$, which are $X^{r_1+r_2}$ or X^{2r_2}. We thus get $2e = 2r_2 - 2r_1 \in \{r_1 + r_2, 2r_2\}$, which give $r_2 = 3r_1$ or $r_2 = 2r_1$, respectively, none of which is possible since we just established that $r_2 > 3r_1$. So, X^{2e} cannot appear in $R(X)^2$.

Well, that is only possible if $R(X)$ itself contains with a nonzero coefficient λ the monomial X^f such that $\delta^2 X^{2e}$ appearing in $R(X)^2$ is eliminated by the cross term $2\lambda X^{r_1+r_2+f}$ of $R(X)^2$. Comparing degrees we get $r_1 + r_2 + f = 2e = 2r_2 - 2r_1$, so $f = r_2 - 3r_1$. However, since $f \geq 2r_1$, we get $r_2 - 3r_1 \geq 2r_1$, so $r_2 \geq 5r_1$, a contradiction since $r_2 \leq 4r_1$. Hence, this case cannot appear.

Thus, the only possibility is $(r_1, r_2) = (1, 3)$. Since $r_1 = 1$, it follows that $s_1 = 0$. Thus,

$$\begin{aligned} P_{r_1,r_2,s_1,s_2}(X) &= P_{1,3,0,s_2}(X) = (X^2-1)(\alpha^{s_2}X^6 - \beta^{s_2}) + 5X^4 \\ &= \alpha^{-s_2}((X^2-1)(\alpha^{2s_2}X^6 - (-1)^{s_2}) + 5\alpha^{s_2}X^4). \end{aligned}$$

We thus took

$$P_\zeta(X, Y) = (X^2-1)(Y^2X^6 - \zeta) + 5YX^4 \quad \text{for} \quad \zeta \in \{\pm 1\}.$$

We computed the derivative of $P_\zeta(X, Y)$ with respect to X and computed the resultant, with respect to the variable X, of this polynomial with $P_\zeta(X, Y)$. We got

$$Q_\zeta(Y) := \mathrm{Res}_X \left(P_\zeta(X, Y), \frac{\partial P_\zeta}{\partial X}(X, Y) \right).$$

So, the roots of $Q_\zeta(Y)$ are exactly the values of Y for which $P_\zeta(X, Y)$ has a double root as a polynomial in X. It turns out when $\zeta = 1$, the only roots of $Q_1(Y)$ are zero, and the roots of an irreducible polynomial of degree 4, so such roots are not powers of α of some integer exponent s_2. However, when $\zeta = -1$, we have that

$$Q_{-1}(Y) = -256Y^{12}(Y^2 - 29Y - 1)^2(27Y^2 - 527Y - 27)^2,$$

and we recognize that α^7 and β^7 are roots of $Q_{-1}(Y)$. The other factor $27X^2 - 527X - 27$ has roots which are not algebraic integers, so they cannot be α^{s_2}. So, $s_2 \in \{\pm 7\}$. However,

$$P_{-1}(X, \alpha^7) = (X^2 - \beta^4)^2 G(X),$$

where

$$G(X) = \alpha^{14}X^4 - (\alpha^{13} + \alpha^9)X^2 - \alpha^8$$

is an irreducible polynomial of degree 4 in $\mathbb{K}[X]$. Replacing α^7 by β^7 above gives the conjugate of $P_{-1}(X^7, \alpha^7)$ in $\mathbb{K}[X]$. Thus, $P_{r_1,r_2,s_1,s_2}(X)$ does not have all its roots of even multiplicity.

THANK YOU!