Troisième Rencontre Internationale sur les Polynômes à Valeurs Entières

Rencontre organisée par :
Sabine Evrard

29 novembre-3 décembre 2010

Giulio Peruginelli

Parametrization of integral values of polynomials

Vol. 2, n° 2 (2010), p. 41-49.

<http://acirm.cedram.org/item?id=ACIRM_2010__2_2_41_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

Actes des rencontres du C.I.R.M.
Vol. **2** n° 2 (2010) 41-49

Parametrization of integral values of polynomials

Giulio Peruginelli

Abstract

We will recall a recent result about the classification of those polynomial in one variable with rational coefficients whose image over the integer is equal to the image of an integer coefficients polynomial in possibly many variables. These set is polynomially generated over the integers by a family of polynomials whose denominator is 2 and they have a symmetry with respect to a particular axis.

We will also give a description of the linear factors of the bivariate separated polynomial $f(X) - f(Y)$ over a number field K, which we need to formulate a conjecture for a generalization of the previous result over a generic number field.

1. Introduction

It is classically well-known that the set of pythagorean triples in $\mathbb{Z}^3$ can be obtained as the image of two 3-uples of polynomials in 3 variables with integer coefficients, as far as the variables range through the integers. So it is quite natural to ask if a parametrization of the pythagorean triples is possible using only one 3-uples of polynomials with integer coefficients in some number m of variables. In 2008, Frisch and Vaserstein [FV] proved that this cannot be done, but if we consider polynomials with rational coefficients we get a parametrization:

Theorem 1.1 (Frisch-Vaserstein, 2008)**.** *Let $\mathbb{P} = \{ (x, y, z) \in \mathbb{Z}^3 \mid x^2 + y^2 = z^2 \}$ be the set of pythagorean triples. Then whatever $m \in \mathbb{N}$ it does not exist $\underline{p} = (p_1, p_2, p_3) \in (\mathbb{Z}[T_1, \dots, T_m])^3$ such that*

$$\mathbb{P} = \underline{p}(\mathbb{Z}^m).$$

On the other hand there exists $\underline{f} = (f_1, f_2, f_3) \in (\mathbb{Q}[T_1, \dots, T_4])^3$ such that

$$\mathbb{P} = \underline{f}(\mathbb{Z}^4).$$

Their result is completely explicit (see [FV] for details). In particular the polynomials f_i are integer-valued, that is $f_i(\mathbb{Z}^4) \subset \mathbb{Z}$. As usual we set

$$\mathrm{Int}(\mathbb{Z}^m) = \{f \in \mathbb{Q}[X_1, \dots, X_m] \mid f(\mathbb{Z}^m) \subset \mathbb{Z}\}.$$

Inspired by that result we give the following definitions:

Definition 1.1. *Let $k \geq 1$ and $S \subset \mathbb{Z}^k$. We say that:*

Text presented during the meeting "Third International Meeting on Integer-Valued Polynomials" organized by Sabine Evrard. 29 novembre-3 décembre 2010, C.I.R.M. (Luminy).
2000 *Mathematics Subject Classification.* 11D85, 11C08, 13F20.
Key words. Integer-valued polynomial, image of a polynomial, linear factor bivariate separated polynomial.
The research has been supported by a grant of CNRS, during a visit of the author at the UMR 6140, LAMFA, Amiens.

- S *is* $\mathbb{Z}$-***parametrizable*** *if there exists* $\underline{p} = (p_1, \ldots, p_k) \in (\mathbb{Z}[T_1, \ldots, T_m])^k$ *for some* m *such that* $S = \underline{p}(\mathbb{Z}^m)$.
- S *is* $\mathrm{Int}(\mathbb{Z})$-***parametrizable*** *if there exists* $\underline{f} = (f_1, \ldots, f_k) \in \mathrm{Int}(\mathbb{Z}^m)^k$ *for some* m *such that* $S = \underline{f}(\mathbb{Z}^m)$.

So we may say that the set of pythagorean triples is $\mathrm{Int}(\mathbb{Z})$-parametrizable but not $\mathbb{Z}$-parametrizable, and this is the first example of such a situation. If we consider the integer image of a rational coefficient polynomial (not necessarily integer-valued) we have this result:

Theorem 1.2 (Frisch, 2008)**.** *Let* $h \in \mathbb{Q}[X]$ *be such that* $S = h(\mathbb{Z}) \cap \mathbb{Z} \neq \emptyset$. *Then there exists* $f \in \mathrm{Int}(\mathbb{Z}^m)$, *for some* $m \geq 1$, *such that*

$$S = f(\mathbb{Z}^m).$$

Unfortunately the result is not effective, and if we let the common denominator of the coefficients of $h(X)$ tend to infinity, then the number of variables m of the integer-valued polynomial $f(X_1, \ldots, X_m)$ tends to infinity as well. According to the above terminology, the integer image of a rational coefficients polynomial is $\mathrm{Int}(\mathbb{Z})$-parametrizable.

Following these results we focus our attention on those integer-valued polynomials in one variable whose image is $\mathbb{Z}$-parametrizable, that means it is equal to the image of an integer-coefficients polynomial in possibly many variables. In [PZ] we classify such polynomials, in section 2 we will recall that result, showing that they are polynomially generated by the family of polynomials $B_\beta(X) = p^k X(p^k X - r)/2$, for p odd prime and r odd integer, not divisible by p. We will also recall the crucial result in order to obtain that classification (see proposition 2.1): given a rational coefficient polynomial $f(X)$ such that for every $n \in \mathbb{N}$ there exists $q_n \in \mathbb{Q}$, $q_n \neq n$, such that $f(n) = f(q_n)$, then the curve $\{f(Y) - f(X) = 0\}$ has a non trivial linear factor where all the points (n, q_n) except finitely many lie. More generally, given a number field K with ring of integers O_K, an integral-valued polynomial $f \in K[X]$ such that for infinitely many $\alpha \in O_K$ there exists $q_\alpha \in K$, $q_\alpha \neq \alpha$, such that $f(\alpha) = f(q_\alpha)$ we conjecture that the quasi-integral set of points $\{(\alpha, q_\alpha)\}$ (with that I mean that the q_α's have a common denominator) of the bivariate separated curve $f(X) = f(Y)$ lie in its linear components, except for finitely many exceptions.

In section 3 we give a description of the structure of the linear factors of $f(X) - f(Y)$, showing that the set of their X-leading coefficients form a finite cyclic subgroup of K^*, made by roots of unity. In section 4 we give an easy technical result about sums of roots of unity, which we need to define a family of integer-valued polynomials in the last section. Finally in section 5 we will define a family of polynomials $B_{n,\beta}(X)$ which are a generalization of the previous polynomials in the rational case. We conjecture that these polynomials polynomially generate over O_K the set of integral-valued polynomial whose image is O_K-parametrizable.

2. Main result

First we define a family of integer-valued polynomials, which polynomially generate the set of integer-valued polynomials whose image is $\mathbb{Z}$-parametrizable.

Let $\beta \in \mathbb{Q}$, $\beta = \frac{r}{s}$, with r, s odd coprime integers and $s > 0$.

$$B_\beta(X) \doteq \frac{sX(sX - r)}{2}$$

The above polynomials enjoy these properties:

1) $B_\beta(X) = B_\beta(-X + \beta)$
2) $B_\beta \in \mathrm{Int}(\mathbb{Z})$

We can rephrase the first one into the following one:

1') $B_\beta(Y) - B_\beta(X) = \frac{s^2}{2}(Y - X)(Y + X - \beta)$

that is, the bivariate separated polynomial $B_\beta(Y) - B_\beta(X)$ has a non trivial linear factor, $Y + X - \beta$.
Moreover, if we add the condition that s is a prime power, that is $s = p^k$, for some $k = 0, 1, \ldots$, their images can be parametrized with an integer-coefficients polynomial (we can easily check that by direct computation):

- given $B_\beta(X)$, β odd integer, we set $g_\beta(X) \doteqdot B_\beta(2X)$; then we have $g_\beta \in \mathbb{Z}[X]$ and $B_\beta(\mathbb{Z}) = g_\beta(\mathbb{Z})$.

- given $B_\beta(X)$, $\beta = r/p^k$, $k \geq 1$ with r and p coprime odd integers and p prime, then if we set
$$g_\beta(X_1, X_2) \doteqdot B_\beta(2X_1 + (\beta - 1)(1 - X_2^{k(p-1)})^k)$$
we have that $g_\beta \in \mathbb{Z}[X_1, X_2]$ and $B_\beta(\mathbb{Z}) = g_\beta(\mathbb{Z}^2)$.

Given $B_\beta(X)$ and g_β as above, if $F \in \mathbb{Z}[X]$ we have that $F(B_\beta(\mathbb{Z})) = F(g_\beta(\mathbb{Z}^m))$, where $m = 1$ or 2 according to the fact that $\beta \in \mathbb{Z}$ or $\beta \in \mathbb{Q} \setminus \mathbb{Z}$, respectively. So every element in the ring $\mathbb{Z}[B_\beta(X)]$ is an integer-valued polynomial whose image is $\mathbb{Z}$-parametrizable. As the following theorem shows, these are the only ones. We may say that the family of polynomials $\{B_\beta(X)\}$ polynomially generates over $\mathbb{Z}$ all integer-valued polynomials with this property.

Theorem 2.1 (P. - Zannier, 2010)**.** *Let $f \in$Int$(\mathbb{Z})$, $f \notin \mathbb{Z}[X]$.*
Then $f(\mathbb{Z}) = g(\mathbb{Z}^m)$ for some $m \in \mathbb{N}$ and $g \in \mathbb{Z}[X_1, \ldots, X_m]$ if and only if $f \in \mathbb{Z}[B_\beta(X)]$ for some $\beta = \frac{r}{s} \in \mathbb{Q}$ such that

- *r and s are odd coprime integers*
- *$s = p^k$, where p is prime and $k \geq 0$.*

Moreover if that happens, we can choose $m \in \{1, 2\}$, m is equal to 1 if and only if $\beta \in \mathbb{Z}$.

We remark that if such a parametrization exists, then it can be explicitly made as shown above with a polynomial which has at most two variables. Note also that the common denominator of an integer-valued polynomial whose image is $\mathbb{Z}$-parametrizable is a power of the prime 2 and no other prime factor can appear in the denominator. As the next proposition will show, that is related to the number of roots of unity in $\mathbb{Q}$.

In [PZ] the following crucial proposition is proved.

Proposition 2.1. *Let $f \in \mathbb{Q}[X]$ be not constant. If for infinitely many integers $n \in \mathbb{N}$ there exists $q = q_n \in \mathbb{Q}$ such that $f(q) = f(n)$ and $q \neq n$, then there exists a unique $\beta \in \mathbb{Q}$ such that $f(X) = f(\beta - X)$. Moreover $q_n = -n + \beta$ for all but finitely many such n.*

This means that $X + Y - \beta$ is a linear factor of the bivariate separated polynomial $f(X) - f(Y)$ (remember that $X - Y$ is always a linear factor of such a polynomial); moreover the points (n, q_n) of the curve $f(X) = f(Y)$ lie in that linear component, except for finitely many exceptions. We recall the main steps of the proof of the main theorem.

Since $f(\mathbb{Z}) \supset g(\mathbb{Z}^m)$ then by Hilbert Irreducibility Theorem there exists a polynomial $L \in \mathbb{Q}[\underline{X}]$ such that $f(L(\underline{X})) = g(\underline{X})$, so f and g are algebraically related (see next section and especially proposition 3.1, for another interpretation of this situation). Moreover since g has integer coefficients and f has not, by theorem 3.1 of [PZ] we have that the integer image of L, that is $L(\mathbb{Z}^m) \cap \mathbb{Z}$, is contained in a single residue class modulo p, where p is any prime which divides the common denominator of f.

From the other inclusion $f(\mathbb{Z}) \subset g(\mathbb{Z}^m)$ we have that for all $n \in \mathbb{Z}$ there exists $\underline{x}_n \in \mathbb{Z}^m$ such that

$$f(n) = g(\underline{x}_n) = f(L(\underline{x}_n))$$

so that $(n, L(\underline{x}_n)) \in \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) \mid f(x) - f(y) = 0\}$.

By proposition 2.1 above, for n sufficiently large we have that $(n, L(\underline{x}_n))$ annihilate the linear factors of $f(X)-f(Y)$. Since over $\mathbb{Q}$ the number of these factors is at most 2, which is the number of roots of unity in $\mathbb{Q}$ (see also next section), and by the aforementioned result of theorem 3.1 of [PZ] there must be two linear factors and p is forced to be equal to 2. For more details see [PZ].

We conjecture that over a number field K with ring of integers O_K the situation is analogous; in that case we can have more than two linear components for the curve $f(X) = f(Y)$, if the field K contains roots of unity other than ± 1. So in general the q's may distribute among several linear components, which for symmetry reasons are strictly related one to each other, in such a way that, by a slight abuse of language, they form a finite cyclic group (see section 3 for a study of linear factors of a bivariate separated polynomials $f(Y) - f(X)$ over a generic number field).

Conjecture 2.1. *Let $f \in K[X]$ be not constant. If for infinitely many integers $\alpha \in O_K$ there exists $q = q_\alpha \in K$ such that $f(q) = f(\alpha)$ and $q \neq \alpha$, then there exists a unique pair (ξ, β), where ξ is a root of unity and $\beta \in K$ such that $f(X) = f(\xi X + \beta)$.*
Moreover $\{q_\alpha\}_\alpha \subset \bigcup_{i=1}^{n-1} \{\xi^i \alpha + \beta_i\}_\alpha$ (except for finitely many of such α's) where $\beta_1 = \beta$ and $\beta_i = \beta_1(\sum_{j=0,\dots,i-1} \xi^j)$.

In other words, if we consider the curve $C = C_f = \{(x, y) | f(x) = f(y)\}$, then the points (α, q_α) of this curve lie on the linear components of C, $Y - (\xi^i X + \beta_i) = 0$. Note that in the case $K = \mathbb{Q}$ we obtain proposition 2.1.

3. Linear factors of $f(X) - f(Y)$

Let K be a number field and $f \in K[X]$. We want to describe the Y-linear factors that the polynomial $F(X, Y) = f(Y) - f(X) \in K[X, Y]$ has over K. These correspond to the roots of $F(X, Y)$ over $K[X]$.

Suppose that $Y - Q(X)$ is such a factor (of course $Q(X) \in K[X]$, since F is monic in Y over $K[X]$, which is integrally closed); this means that $f(Q(X)) = f(X)$ so in particular $Q(X)$ has degree 1, let us say $Q(X) = cX + \beta_1$, where $c, \beta_1 \in K$. By looking at the leading terms of the last equation we deduce that $c = \xi$ is a root of unity of order dividing the degree d of f. Let us suppose that $\xi = \xi_n$ has primitive order n. Since $f(X) = f(\xi X + \beta_1)$ by iterating this formula we have that

$$f(X) = f(\xi X + \beta_1) = f(\xi^2 X + \beta_2) = \dots = f(\xi^i X + \beta_i) = \dots = f(\xi^{n-1} X + \beta_{n-1})$$

where $\beta_i = \beta_1(\sum_{0 \leq j \leq i-1} \xi^j)$, for $i = 2, \dots, n$, so that each β_i for $i \geq 2$ is uniquely determined by β_1 (and by the root of unity ξ). Note that $\beta_n = 0$ and the set $\{\beta_i\}_{i=1,\dots,n}$ has n distinct elements (for a detailed proof of that see next section, lemma 4.1). We summarize these remarks in the following lemma:

Lemma 3.1. *Let $f \in K[X]$ be a polynomial of degree d. Then every Y-linear factor of $f(Y) - f(X)$ over K is of the form $Y - (\xi X + \beta)$, for some $\beta, \xi \in K$ where ξ is a root of unity of order n which is a divisor of d. In particular if $Y - (\xi X + \beta)$ is such a factor, $\{Y - (\xi^i X + \beta_i)\}_{i=1,\dots,n}$ are linear factors of $f(Y) - f(X)$, where $\beta_i = \beta_1(\sum_{0 \leq j \leq i-1} \xi^j)$ is uniquely determined by $\beta_1 = \beta$ and ξ.*

Note that the lemma includes also the trivial case of the linear factor $Y - X$ of $f(Y) - f(X)$. Moreover since the polynomial $F(X, Y)$ is separable, each of its factors appears with multiciplicity

1. From now on we will denote by T the set of roots of $F(X,Y)$ over $K[X]$; by the above considerations, these are polynomials of the kind $\xi X+\beta$, with $\beta,\xi\in K$, ξ being a root of unity. Next lemmata will show that T is indeed made by a single group of linear factors, that is, given $\xi X+\beta,\xi' X+\beta'\in T$, we have that $\xi'=\xi^i$ and $\beta'=\beta_i$, for some $i\in\{1,\dots,n\}$. We denote by $\mathrm{lc}(f)$ the leading coefficient of a polynomial $f\in K[X]$.

Lemma 3.2. *The set*

$$\mathcal{L}=\{\ \mathrm{lc}(f)\mid f\in T\}$$

is a finite (hence cyclic) group of K^*.

Proof : First of all $\mathcal{L}$ is a finite set because so is the number of linear factors of $f(Y)-f(X)$. It is also not empty because for each polynomial f we always have that $Y-X$ divides $f(Y)-f(X)$, so that $1\in\mathcal{L}$. And if we have

$$f(X)=f(\xi X+\beta)=f(\xi' X+\beta')$$

where ξ,ξ' are roots of unity, then we also have that

$$f(X)=f(\xi\xi' X+\xi\beta'+\beta)$$

so that $Y-(\xi\xi' X+\xi\beta'+\beta)$ is a linear factor of $f(Y)-f(X)$. In the same way we prove that if $\xi\in\mathcal{L}$ then $\xi^{-1}\in\mathcal{L}$. □

Therefore, with a little abuse of language, we can say that the set of linear factors of $f(X)-f(Y)$ form a finite cyclic group. The following lemma is easy to prove.

Lemma 3.3. *If ξ is a root of unity of order n and $\beta,\beta'\in K$ are such that*

$$f(X)=f(\xi X+\beta)=f(\xi X+\beta')$$

then $\beta=\beta'$.

Proof : if $f(X)=a_dX^d+a_{d-1}X^{d-1}+\dots$, then the leading term of $f(\xi X+\beta)-f(\xi X+\beta')$ is $d\xi^{d-1}(\beta-\beta')X^{d-1}$. If $d\xi^{d-1}(\beta-\beta')=0$ then $\beta=\beta'$. □

This implies that the map $T\to\mathcal{L}$, which associates to $\xi X+\beta$ its coefficient ξ, is indeed a bijection. In the same way we prove (using the fact that the $\sum_{0\le j\le i-1}\xi_n^j$, for $i=0,\dots,n-1$ are n distinct elements, see next section, lemma 4.1):

Lemma 3.4. *If ξ,ξ' are roots of unity and $\beta\in K$ are such that*

$$f(X)=f(\xi X+\beta)=f(\xi' X+\beta)$$

then $\xi=\xi'$.

Suppose now that $f(O_K)=g(O_K^m)$, for some $g\in O_K[X_1,\dots,X_m]$. Let us write down the factorization over K of the polynomials $f(Y)-f(X)$ and $f(Y)-g(X_1,\dots,X_m)=f(Y)-g(\underline{X})$:

$$f(Y)-f(X)=B(X,Y)\prod_{i=1}^{n}(Y-(\xi_n^i X+\beta_i)) \tag{3.1}$$

$$f(Y)-g(\underline{X})=Q(\underline{X},Y)\prod_{j=1}^{k}(Y-L_j(\underline{X})) \tag{3.2}$$

where $B(X,Y)$ is the product of all the irreducible factors of Y-degree greater or equal to 2 and the same for $Q(\underline{X},Y)$ (note that $k\ge 1$ by Hilbert Irreducibility Theorem). We want to compare the linear factors which appears in (3.1) on with the linear factors in (3.2). We denote

as before with T the set of roots of $f(Y)-f(X)$ in $K[X]$, and we denote by Ω the set of roots of $f(Y)-g(\underline{X})$ in $K[\underline{X}]$:

$$T \doteqdot \{\xi_n^i X+\beta_i\}_{i=1,\dots,n}$$
$$\Omega \doteqdot \{L_j(\underline{X})\}_{j=1,\dots,k}$$

The next proposition shows that there is a bijection between T and Ω, or equivalently $n=k$.

Proposition 3.1. *Suppose that $f(O_K)=g(O_K^m)$, for some $g\in O_K[X_1,\dots,X_m]$. Then the number of Y-linear factors in the factorization over K of $f(Y)-f(X)$ is equal to the number of Y-linear factors in the factorization over K of $f(Y)-g(\underline{X})$.*

So under the (important!) assumption that f and g share the same image over the integers, the number of Y-linear factors of $f(Y)-f(X)$ and $f(Y)-g(\underline{X})$ is the same.

Proof : as we said, it follows from Hilbert Irreducibility Theorem that Ω is not empty; let us fix $L_1(\underline{X})\in\Omega$. Let us denote $l_i(X)=\xi^i X+\beta_i$, for $i=1,\dots,n$. Let us define the following application

$$\begin{aligned}\Phi :& T\to\Omega\\ & l_i(X)\mapsto l_i(L_1(\underline{X}))=\xi^i L_1(\underline{X})+\beta_i\end{aligned}$$

The map Φ is well defined: $f(X)=f(l_i(X))$ implies $f(L_1(\underline{X}))=f(l_i(L_1(\underline{X})))$ and $g(\underline{X})=f(L_1(\underline{X}))$.
Injectivity: if $\Phi(l_{i_1})=\Phi(l_{i_2})$ then $\xi_{i_1}L_1+\beta_{i_1}=\xi_{i_2}L_1+\beta_{i_2}$. If $\xi_{i_1}\neq\xi_{i_2}$ then we have $L_1=(\beta_2-\beta_1)/(\xi_{i_1}-\xi_{i_2})$, which is constant, contradiction. So we have that $\xi_{i_1}=\xi_{i_2}$ which implies $l_{i_1}=l_{i_2}$.
Surjectivity: it follows from the next proposition: if $L\in\Omega$, $L\neq L_1$ then $L=\xi L_1+\beta$, for some root of unity ξ in K and $\beta\in K$ such that $f(X)=f(\xi X+\beta)$. Then $\Phi(\xi X+\beta)=L$. □

The following proposition is a generalization of proposition 2.2 of [PZ] and the proof is exactly the same as the one which appears in [PZ].

Proposition 3.2. *Let $f\in K[X]$ be nonconstant and let $R,S\in K[\underline{X}]$ be also nonconstant and such that $f(R)=f(S)$. Then either $R=S$ or $R=\xi S+\beta$ for some root of unity ξ in K and $\beta\in K$ such that $f(X)=f(\xi X+\beta)$ identically, and in this case β is uniquely determined by f.*

4. Sums of roots of unity

Let $\xi=\xi_n$ be a primitive root of unity in K of order n. We define

$$\zeta_i \doteqdot \sum_{j=0}^{i-1}\xi^j$$

for $i=1,\dots,n$. These are elements of the ring of integers O_K of K. Note that $\zeta_n=0$.

We need the following lemma, the proof is due to Chirivi.

Lemma 4.1. *For each $i<n$ we have that $\zeta_i\neq 0$.*

Proof : Without loss of generality we may suppose that $\xi=e^{2\pi i/n}$. Suppose by contradiction that there exists $d>0$ such that $\zeta_d=0$; let such a d be the minimum with that property. Write $n=qd+r$ with $0\le r<d$. If $0<r$ then

$$0=\zeta_n=\zeta_d(1+\xi^d+\xi^{2d}+\ldots+\xi^{qd})+\xi^{qd}\zeta_r$$

since $\zeta_d = 0$ then $\zeta_r = 0$ but this is not possible since d is the minimum with that property. So $d|n$, which in particular implies that $d \leq n/2$. Then $\mathrm{Im}(\xi^k) > 0$ for each $0 < k < d$, because ξ^k lies in the upper plane, so $\mathrm{Im}(\zeta_d) > 0$ unless $d = 1$. But in that case $\zeta_1 = 1 \neq 0$. □

We also have the following relations (suppose $i > k$), which can be proved directly:

$$\zeta_i - \zeta_k = \xi^k \zeta_{i-k} \tag{4.1}$$

$$\xi\zeta_i = \zeta_{i+1} - 1 \tag{4.2}$$

Let v be a finite valuation of K; note that $\zeta_i \in O_v$, the valuation ring of v. Let us define

$$\imath = \imath(v, \xi_n) \doteqdot \min\{i \in \{1, \ldots, n\} \mid v(\zeta_i) > 0\}.$$

Note that this minimum exists, since $\zeta_n = 0$; moreover by construction we obviously have that $2 \leq \imath \leq n$. We have that

Properties

i) if $i_1 \neq i_2 \in \{1, \ldots, \imath\}$, then $\zeta_{i_1} \not\equiv \zeta_{i_2} \pmod{v}$ (that is $v(\zeta_{i_1} - \zeta_{i_2}) = 0$).
ii) $v(\zeta_{k\imath}) > 0$ for each $k > 0$,
iii) if $i \in \{1, \ldots, \imath - 1\}$ then $\zeta_i \equiv \zeta_{k\imath+i} \pmod{v}$ for each $k > 0$,
iv) $\imath$ divides n.

To prove i) we suppose $i_1 < i_2$; it is sufficient to note that $\zeta_{i_2} - \zeta_{i_1} = \xi^{i_1}\zeta_{i_2-i_1}$, by (4.1). If $v(\zeta_{i_1} - \zeta_{i_2}) > 0$ then $v(\zeta_{i_2-i_1}) > 0$ but this is not possible since $0 < i_2 - i_1 < \imath$.
To prove ii), we note that $\zeta_\imath \equiv 0 \pmod{v} \Rightarrow \xi\zeta_\imath \equiv 0 \pmod{v}$, so $\zeta_{\imath+1} - 1 \equiv 0 \pmod{v}$ by (4.2) above. We get

$$\begin{aligned}
\zeta_{\imath+1} \equiv 1 = \zeta_1 &\pmod{v} \\
\xi\zeta_{\imath+1} \equiv \xi\zeta_1 &\pmod{v} \\
\zeta_{\imath+2} - 1 \equiv \zeta_2 - 1 &\pmod{v} \\
\zeta_{\imath+2} \equiv \zeta_2 &\pmod{v} \\
&\cdots \\
\zeta_{\imath+h} \equiv \zeta_h &\pmod{v}
\end{aligned}$$

for each $h = 1, \ldots, \imath - 1$. Hence it follows $\zeta_{k\imath} \equiv \zeta_\imath \equiv 0 \pmod{v}$. In the same way we prove iii). Finally for property iv), let $n = q\imath + r$, with $0 \leq r < \imath$. Since $0 = \zeta_n = \zeta_{q\imath+r} \equiv \zeta_r \pmod{v}$ by iii), this implies $r = 0$, by minimality of $\imath$.

In particular property i) implies that there are exactly $\imath$ distinct residue classes modulo v among the $\{\zeta_i\}_{i=1,\ldots,n}$, so that we always have $\imath \leq N(v)$, where $N(v)$ is the cardinality of the residue field of v.

5. A family of bivariate separated polynomials with n distinct linear factors

Let v be a finite valuation of a number field K with uniformizer π, and let us denote α_v the residue of an integral element $\alpha \in O_K$ modulo v. Given γ_1 a v-unit, that is $v(\gamma_1) = 0$, and $\xi = \xi_n$ a primitive n-th root of unity in K, we define

$$\gamma_i \doteqdot \zeta_i\gamma_1 = (\sum_{j=0}^{i-1} \xi^j)\gamma_1$$

for $i = 1, \dots, n$. Note that $\gamma_n = 0$. By properties i) and iii) of the previous section we have that

$$\imath(v, \xi_n) = \#\{(\gamma_i)_v\}_{i=1,\dots,n}.$$

We define the following family of polynomials in $K[X]$, where $\beta \doteqdot \gamma_1/\gamma$, γ is another v-unit:

$$B_{n,\beta}(X) \doteqdot \frac{1}{\pi}\prod_{i=1}^{n}(\gamma X - \gamma_i). \tag{5.1}$$

Note that by construction we have that

$$B_{n,\beta}(X) = B_{n,\beta}(\xi^i X + \beta_i) \tag{5.2}$$

where $\beta_i = \gamma_i/\gamma$, for $i = 1, \dots, n$. Note again that this last property corresponds to the fact that $B_{n,\beta}(Y) - B_{n,\beta}(X)$ has exactly n linear factors, namely $Y - (\xi^i X + \beta_i)$.

From now on we suppose that O_K is a unique factorization domain, so in particular we may suppose $\pi, \gamma, \gamma_1 \in O_K$. In this way the polynomial $B_{n,\beta}(X)$ is written as a ratio of a polynomial in $O_K[X]$ over a non-zero element of O_K. Under this assumption we have that

Lemma 5.1. *$B_{n,\beta}(X) \in \mathrm{Int}(O_K)$ if and only if $\imath(v, \xi_n) = N(v)$.*

Proof : This follows from $\imath(v, \xi_n) \leq N(v)$ and the fact that $\imath(v, \xi_n) = \#\{(\beta_i)_v\} = \#\{(\gamma_i)_v\}$, as we have just seen (more precisely there are $\imath$ distinct residue classes modulo v of such β_i's and by definition there are $N(v)$ residue classes modulo v). If $\imath < N(v)$ (as for example when the order n of ξ is less than the cardinality $N(v)$ of the residue field at v so that $\imath(v, \xi_n) \leq n < N(v)$) the polynomials $B_{\beta,n}(X)$ are not integer-valued, since there are elements of O_K which are sent by the numerator of the polynomial $B_{n,\beta}$ into elements which are not congruent to zero modulo π (just pick up an element in the remaining $N(v) - \imath(v, \xi_n)$ residue classes modulo v). Note that the multiplication by a v-unit γ has the effect to permute the residue classes modulo v, so we immediately see from the definition of the polynomials $B_{n,\beta}(X)$ in (5.1) that they are integral-valued if and only if $\{\gamma_i\}_{i=1,\dots,n}$ covers all the $N(v)$ residue classes modulo v.□

Note that the condition of the lemma is satisfied in the rational case for the root of unity -1 only for the valuation 2, as we have already seen in the second section.

Given a polynomial $f \in K[X]$ we denote by Ω_f the finite set of finite valuation v of K such that the Gauss norm $\| \ \|_v$ relative to v of f is greater than 1. As usual ξ_n denotes a primitive n-th root of unity and $\mathcal{M}_v$ the maximal ideal of O_K associated to v.

Conjecture 5.1. *Let K be a number field such that O_K is a unique factorization domain. Let $f \in \mathrm{Int}(O_K)$, $f \notin O_K[X]$. Then $f(O_K)$ is O_K-parametrizable if and only if there exist $\xi_n \in K$, $\gamma, \gamma_1 \in O_K \setminus \mathcal{M}_v$ for some $v \in \Omega_f$ such that $f \in O_K[B_{n,\beta}(X)]$ with $\beta = \gamma_1/\gamma$ and moreover*

- *for such a v we have $\imath(v, \xi_n) = N(v) \leq n$*
- *the number of finite valuation v of K such that $v(\gamma) < 0$ is less than n.*

We believe that the if part should be relatively easy to prove. For example in the case $\gamma \in O_K^*$ (a global unity), we have that $B_{n,\beta}(\pi X)$ parametrizes the integral values of $B_{n,\beta}(X)$. If γ is not in O_K^* we are forced to look for a polynomial in more than one variable to parametrize the integral values of $B_{n,\beta}$.

Acknowledgments. I wish to warmly thank all the integer-valued research group of Amiens: Jacques Boulanger, Jean-Luc Chabert, Sabine Evrard and Youssef Fares. I had several discussion with them which helped me to improve the exposition of my results. I thank also the anonymous referee for several suggestions he gave.

References

[CC] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys and Monographs, 48, Providence, 1997.

[F] S. Frisch, *Remarks on polynomial parametrization of sets of integer points*, Comm. Algebra 36 (2008), no. 3, 1110-1114.

[FV] S. Frisch, L. Vaserstein, *Parametrization of Pythagorean triples by a single triple of polynomials*, Pure Appl. Algebra 212 (2008), no. 1, 271-274.

[PZ] G. Peruginelli, U. Zannier, *Parametrizing over $\mathbb{Z}$ integral values of polynomials over $\mathbb{Q}$*, Comm. Algebra 38 (2010), no. 1, 119–130.

Institut für Analysis und Comput. Number Theory, Technische Univ. Graz, Steyrergasse 30, A-8010 Graz, Austria. • peruginelli@math.tugraz.at