LE MATEMATICHE
Vol. LXIX (2014) – Fasc. I, pp. 159–168
doi: 10.4418/2014.69.1.11

PRIME INJECTIONS AND QUASIPOLARITIES

OCTAVIO A. AGUSTÍN-AQUINO

Let p be a prime number. Consider the injection

$$\iota : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/pn\mathbb{Z} : x \mapsto px,$$

and the elements $e^u.v := (u,v) \in \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}^\times$ and $e^w.r := (w,r) \in \mathbb{Z}/pn\mathbb{Z} \rtimes \mathbb{Z}/pn\mathbb{Z}^\times$. Suppose that $e^u.v \in \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}^\times$ is seen as an automorphism of $\mathbb{Z}/n\mathbb{Z}$ defined by $e^u.v(x) = vx + u$; then $e^u.v$ is a *quasipolarity* if it is an involution without fixed points. In this brief note we give an explicit formula for the number of quasipolarities of $\mathbb{Z}/n\mathbb{Z}$ in terms of the prime decomposition of n, and we prove sufficient conditions such that $(e^w.r) \circ \iota = \iota \circ (e^u.v)$, where $e^w.r$ and $e^u.v$ are quasipolarities.

1. Some preliminaries

Before we can state and prove the results of this paper, a brief exposition of some conventions, notions and notations taken from Guerino Mazzola's monograph on mathematical musicology [5] is in order. First of all, the ring (or $\mathbb{Z}$-module) $\mathbb{Z}/n\mathbb{Z}$ is a good model of the n-tone equally tempered scale modulo octaves [5, Chapter 6, Section 4]. We now consider the group

$$\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) := (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$$

Entrato in redazione: 1 marzo 2013

AMS 2010 Subject Classification: 11A05, 11A07, 11A25.
Keywords: Quasipolarity, injection, unitary divisor.

and let us denote an element $(u,v) \in \mathrm{Aff}(\mathbb{Z}/n\mathbb{Z})$ by $e^u.v$. We have an action of $\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z})$ on $\mathbb{Z}/n\mathbb{Z}$ defined in the following way:

$$e^u.v(x) = vx + u.$$

These notations are meant to exhibit the importance of the actions of affine groups on musical objects. In particular, the exponential notation e^u was chosen because the composition of two translations (or transpositions, musically speaking) is $e^u \circ e^v = e^{u+v}$. The linear part v is also musically meaningful: the best example is perhaps $v = -1$, which corresponds to the inversion of intervals and melodies (but similar interpretations are possible with the rest of the linear parts).

The aforementioned action of $\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z})$ on $\mathbb{Z}/n\mathbb{Z}$ extends naturally to an action on the powerset of $\mathbb{Z}/2k\mathbb{Z}$ in a pointwise manner. A *marked strong dichotomy* is a subset $D \subseteq \mathbb{Z}/2k\mathbb{Z}$ such that there is a unique $\pi = e^u.v$ that satisfies

$$\pi(D) = (\mathbb{Z}/2k\mathbb{Z}) \setminus D.$$

Marked strong dichotomies are important abstractions for the mathematical theory of counterpoint as conceived by Mazzola, because they generalize the notion of consonance and dissonance in the standard 12-tone equal tuning. See [5, Part VII], [1] and [2] for further details.

2. Polarities and quasipolarities

The unique element π that interchanges a marked strong dichotomy D and its complement is called the *polarity* of D. This nomenclature was chosen by Mazzola because:

> [T]he traditional consonance/dissonance concept is not a polar one, since intervals are more or less consonant, for example in Euler theory and Helmholtz theory. But in musical theory, they are strictly separated into one or another category. So what is more or less in the acoustical or number[...] theories is now compressed into two bags, or poles. That is the reason. (Guerino Mazzola, personal communication, September 25th, 2013).

We observe that if we regard π as a automorphism of $\mathbb{Z}/2k\mathbb{Z}$, we have $\pi^2 = \mathrm{Id}_{\mathbb{Z}/2k\mathbb{Z}}$ and it has no fixed points. Thus, any $\pi = e^u.v$ with these two properties is called a *quasipolarity*.

Remark 2.1. From the definition, it is easy to see that the notion of quasipolarity makes sense for $\mathbb{Z}/n\mathbb{Z}$ only when n is even: if π is an involution, then its cycles (regarding it as a permutation) have cardinality at most 2, and none can actually be of cardinality 1, because otherwise π would have a fixed point.

Let $\omega(2k)$ be the number of distinct prime factors of $2k$, with $k \geq 1$, such that

$$2k = 2^{\alpha} \prod_{i=1}^{\omega(2k)-1} p_i^{\alpha_i}$$

is its prime decomposition. Suppose that $2k = 2^{\alpha}ab$ with a coprime with b. It is known [7, p. 191] that the solutions of $v^2 \equiv 1 \pmod{2k}$ are given by the simultaneous solutions of the pair of congruences

$$x \equiv 1 \pmod{2a}, \quad x \equiv -1 \pmod{2b} \tag{1}$$

if $\alpha = 1, 2$, or the two pairs

$$\begin{aligned} x &\equiv 1 \pmod{2^{\alpha-1}a}, \quad x \equiv -1 \pmod{2^{b}}, \\ x &\equiv 1 \pmod{2a}, \quad x \equiv -1 \pmod{2^{\alpha-1}b}, \end{aligned} \tag{2}$$

if $\alpha > 2$. Moreover, in [3, Theorem 3.1] it is proved that the number of affine parts e^u available for an involution v such that $e^u.v$ is a quasipolarity is

$$\frac{2k}{\gcd(v-1, 2k)},$$

whenever

$$2\frac{2k}{\gcd(v+1, 2k)} = \gcd(v-1, 2k). \tag{3}$$

With this information, we can easily compute some values of the number $Q(2k)$ of quasipolarities of $\mathbb{Z}/2k\mathbb{Z}$ for small values of $2k$, see Table 1.

The sequence $Q(2k)$ appears in the On-Line Encyclopedia of Integer Sequences (OEIS) as entry A034448 [6], in relation with a different concept in number theory that we now explain.

Definition 2.2. A divisor d of n is said to be *unitary* if $\gcd(d, \frac{n}{d}) = 1$, and we write $d||n$.

We have the following result that relates unitary divisors and quasipolarities.

Proposition 2.3. *Let $\sigma_1^*(n) := \sum_{d||n} d$ be the sum of the unitary divisors of n. We have*

$$Q(2k) = \sigma_1^*(k).$$

Proof. Suppose first that $\alpha = 1$. We have that v satisfies (1),

$$v \equiv 1 \pmod{2a}, \quad v \equiv -1 \pmod{2b},$$

thus $2a \mid (v-1)$ and $2b \mid (v+1)$. Now

$$\gcd(v-1,2k) = 2a \quad \text{and} \quad \gcd(v+1,2k) = 2b$$

because $2k$ is divisible by 2 only once. This means that

$$2\frac{2k}{\gcd(v+1,2k)} = 2\frac{2ab}{2b} = 2a = \gcd(v-1,2k),$$

which implies that there are exactly

$$\frac{2k}{\gcd(v-1,2k)} = \frac{2ab}{2a} = b$$

quasipolarities of the form $e^u.v$. From this it is evident that each involution v is in bijective correspondence with a unitary divisor b of k, thus

$$Q(2k) = \sum_{v^2 \equiv 1 \pmod{2k}} \frac{2k}{\gcd(v-1,2k)} = \sum_{b||k} b = \sigma_1^*(k).$$

If $\alpha = 2$ the same reasoning works *mutatis mutandis* as long as $\gcd(v-1,2k) = 4a$. Otherwise, $\gcd(v-1,2k) = 2a$, which means that $v-1 = 2q$ with q odd. Then $v+1 = 2(q+1) = 4q'$, hence $\gcd(v+1,2k) = 4b$, which rehabilitates the argument because $2b$ is a unitary divisor of k.

The case $\alpha \geq 3$ is slightly more difficult. The symmetry of the systems of congruences (2) enable us to suppose, without loss of generality, that $\gcd(v-1,2k) = 2^\beta a$, with $\beta \geq \alpha - 1$. If $\gcd(v-1,2k) = 2^\alpha a$, then necessarily $\gcd(v+1,2k) = 2b$, for $v \equiv -1 \pmod{2b}$ and $\gcd(v-1,v+1) = 2$, and therefore the proof goes as before. If $\gcd(v-1,2k) = 2^{\alpha-1}a$, then v does not define quasipolarities, but $w = v+k$ does (we note, in passing, that only one of v and w is divisible by 2^α, for otherwise $k = w-v$ would be divisible by 2^α). Indeed,

$$w^2 = (v+k)^2 = v^2 + 2vk + k^2 = v^2 + 2kv + 2^\alpha kab \equiv v^2 \equiv 1 \pmod{2k},$$

and since $v - 1 = 2^{\alpha-1}aq$ for some odd q then

$$w - 1 = 2^{\alpha-1}aq + k = 2^{\alpha-1}aq + 2^{\alpha-1}ab = 2^{\alpha-1}a(q+b)$$

where $q+b$ is even (it is the sum of two odd integers). Thus $\gcd(w-1,2k) = 2^\alpha a$ and $\gcd(w+1,2k) = 2b$, which yields the summand for b anew. $\square$

Remark 2.4. If the prime decomposition of k is known, we can calculate $\sigma_1^*(k)$ in a more direct way [4]:

$$\sigma_1^*(k) = \prod_{p^u||k} (1+p^u).$$

3. Quasipolarities and injections

In [2, Chapter 4] it is proved that, whenever

1. there is a marked strong dichotomy D in $\mathbb{Z}/2k\mathbb{Z}$ with polarity π and
2. there is a quasipolarity $\pi' \in \mathrm{Aff}(\mathbb{Z}/4k\mathbb{Z})$ such that $\iota \circ \pi = \pi' \circ \iota$ (where $\iota : \mathbb{Z}/2k\mathbb{Z} \to \mathbb{Z}/4k\mathbb{Z}$ is the injection given by $\iota(x) = 2x$),

then π' is the polarity of a marked strong dichotomy D' that contains $2D = \{2x : x \in D\}$ in $\mathbb{Z}/4k\mathbb{Z}$. This means that the notion of consonance (and dissonance) can be meaningfully extended from a $2k$-tone equal tuning to a $4k$-equal tuning; in other words, it is possible to "lift" the original consonances of a $2k$-tone scale to the $4k$-tone scale, in the sense that the lifted polarity restricts to the original polarity in the $2k$-tone scale.

If we were to generalize this result for injections of the form

$$\begin{aligned} \iota : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/pn\mathbb{Z}, \\ x &\mapsto px, \end{aligned}$$

where p is a prime number, we would need first to find the conditions such that $\iota \circ p = p' \circ \iota$, which are the aim of this section.

Suppose that $e^u.v$ is a quasipolarity. As it was noted above, in [3] it is proved that u can be taken as $\frac{2k}{\gcd(v+1,n)}$. Our interest now is to find the conditions such that there exists a quasipolarity $e^w.r : \mathbb{Z}/pn\mathbb{Z} \to \mathbb{Z}/pn\mathbb{Z}$ which renders commutative the following square:

$$\begin{tikzcd} \mathbb{Z}/n\mathbb{Z} \arrow[r, "\iota"] \arrow[d, "e^u.v"'] & \mathbb{Z}/pn\mathbb{Z} \arrow[d, "e^w.r"] \\ \mathbb{Z}/n\mathbb{Z} \arrow[r, "\iota"'] & \mathbb{Z}/pn\mathbb{Z}. \end{tikzcd} \tag{4}$$

We have the following result.

Theorem 3.1. *Let n be an even number, $v \in \mathbb{Z}/n\mathbb{Z}^\times$ an involution, $k = \frac{v^2-1}{n}$ and $u = \frac{n}{\gcd(v+1,n)}$. If either $\gcd(p,2v) \mid k$ or $p \nmid n$, then there exists t such that $r = v + nt$ is an involution in $\mathbb{Z}/pn\mathbb{Z}^\times$. If, additionally, $\frac{r^2-1}{pn}$ is even, then $e^w.r$ is a quasipolarity with $w = pu$ and the diagram (4) commutes.*

Proof. We begin by noting that the square (4) is commutative if and only if

$$w \equiv pu \pmod{pn} \quad \text{and} \quad pr \equiv pv \pmod{pn}.$$

The second congruence is equivalent to $p(r-v) = pnt$ for some integer t. Hence $r - v = nt$ and

$$r = v + nt.$$

Let v be an involution in $\mathbb{Z}/n\mathbb{Z}$. We want r to be an involution. We see that

$$\begin{aligned}(v+nt)^2 &= v^2 + 2vnt + n^2t^2\\ &= 1 + kn + 2vnt + n^2t^2\\ &= 1 + (k + 2vt + nt^2)n,\end{aligned}$$

so, to verify that $(v+nt)$ is an involution, it is necessary and sufficient that $p \mid (k + 2vt + nt^2)$. In other words, t is the solution of the quadratic congruence

$$nt^2 + 2vt + k \equiv 0 \pmod{p}. \tag{5}$$

We distinguish two cases. If $p \mid n$, then it is enough to solve for t the linear congruence

$$2vt \equiv -k \pmod{p}.$$

Such a congruence is solvable if and only if $\gcd(p, 2v) \mid -k$. We note that if $p = 2$, this condition simply means that k must be a multiple of 2.

If $p \nmid n$, the quadratic congruence is unavoidable. Fortunately, $\gcd(2n, p) = 1$ so, in order to solve it, we rewrite (5) to obtain

$$(2nt + 2v)^2 \equiv 4v^2 - 4nk \pmod{p}$$

which reduces to

$$(nt + v)^2 \equiv v^2 - nk \equiv 1 + nk - nk \equiv 1 \pmod{p}.$$

Since 1 is always a quadratic residue, we deduce that $t = n^{-1}(\pm 1 - v)$, where n^{-1} is the inverse of n modulo p.

Suppose now that we have found a t such that $r = v + tn$ is an involution. For there exists w such that $e^w.r$ is a quasipolarity, it is necessary and sufficient to check that

$$2\frac{pn}{\gcd(v + nt + 1, pn)} = \gcd(v + nt - 1, pn). \tag{6}$$

If (6) is true, we can choose

$$w = \frac{pn}{\gcd(v + nt + 1, pn)}. \tag{7}$$

Let us begin. We note that

$$\gcd\left(\frac{v + nt - 1}{2}, \frac{v + nt + 1}{2}\right) = 1$$

and

$$\gcd(v+nt\pm 1, pn) = 2\gcd\left(\frac{v+nt\pm 1}{2}, p\frac{n}{2}\right),$$

thus

$$\begin{aligned}\gcd(v+nt+1, pn)\gcd(v+nt-1, pn) &= 4\gcd\left(\frac{(v+nt)^2-1}{4}, p\frac{n}{2}\right)\\ &= 4\gcd\left(\frac{1+k'pn-1}{4}, p\frac{n}{2}\right)\\ &= 2\gcd\left(\frac{k'pn}{2}, pn\right)\\ &= 2p\gcd\left(k'\frac{n}{2}, n\right).\end{aligned}$$

By observing that

$$\gcd\left(k'\frac{n}{2}, n\right) = n$$

holds if and only if $2 \mid k'$, we conclude that (6) holds if and only if $2 \mid k'$, where $k' = \frac{r^2-1}{pn}$.

To finish the proof, we show that once $e^w.r$ is an involution such that $rp \equiv vp \pmod{pn}$ and w is given by (7), it is true that w equals pu and thus the diagram (4) commutes. If $p \nmid (v+tn+1)$, then

$$\gcd(v+tn+1, pn) = \gcd(v+tn+1, n) = \gcd(v+1, n),$$

which means that

$$w = \frac{pn}{\gcd(v+tn+1, pn)} = \frac{pn}{\gcd(v+1, n)} = pu. \tag{8}$$

We assume now the alternative case $p \mid (v+tn+1)$. Then any common divisor d of $\frac{v+tn+1}{p}$ and n is also a divisor of $v+1$, because $v+1$ is a linear combination of them:

$$v+1 = p\frac{v+tn+1}{p} - tn.$$

It follows that

$$\gcd\left(\frac{v+tn+1}{p}, n\right) \mid \gcd(v+1, n)$$

or, equivalently,

$$\gcd(v+1, n) = \gcd\left(\frac{v+tn+1}{p}, n\right)p = \gcd(v+tn+1, pn).$$

The missing factor is p because any common factor d of $v+1$ and n divides the linear combination $(v+1)+tn$ and also $\frac{(v+1)+tn}{p}$, as long as $\gcd(d,p)=1$ or $d=p^{\lambda-1}$, where p^{λ} is the greatest power of p that divides both $v+tn+1$ and n. In conclusion, equation (8) is true again, and the proof concludes. □

$2k$	$Q(2k)$	Quasipolarities
2	1	$e^1.1$
4	3	$e^2.1, e^1.3, e^3.3$
6	4	$e^3.1, e^1.5, e^3.5, e^5.5$
8	5	$e^4.1, e^1.7, e^3.7, e^5.7, e^7.7$
10	6	$e^5.1, e^1.5, e^3.5, e^5.5, e^7.5, e^9.5$
12	12	$e^6.1, e^2.5, e^6.5, e^{10}.5, e^3.7, e^9.7,$ $e^1.11, e^3.11, e^5.11, e^7.11, e^9.11, e^{11}.11$
14	8	$e^7.1, e^1.13, e^3.13, e^5.13, e^7.13, e^9.13, e^{11}.13, e^{13}.13$
16	9	$e^8.1,$ $e^1.15, e^3.15, e^5.15, e^7.15, e^9.15, e^{11}.15, e^{13}.15, e^{15}.15$
18	10	$e^9.1,$ $e^1.17, e^3.17, e^5.17, e^7.17,$ $e^9.17, e^{11}.17, e^{13}.17, e^{15}.17, e^{17}.17$
20	18	$e^{10}.1, e^2.9, e^6.9, e^{10}.9, e^{14}.9, e^{18}.9, e^5.11, e^{15}.11,$ $e^1.19, e^3.19, e^5.19, e^7.19, e^9.19,$ $e^{11}.19, e^{13}.19, e^{15}.19, e^{17}.19, e^{19}.19$
22	12	$e^{11}.1,$ $e^1.21, e^3.21, e^5.21, e^7.21, e^9.21, e^{11}.21,$ $e^{13}.21, e^{15}.21, e^{17}.21, e^{19}.21, e^{21}.21$
24	20	$e^{12}.1, e^3.7, e^9.7, e^{15}.7, e^{21}.7, e^4.17, e^{12}.17, e^{20}.17,$ $e^1.23, e^3.23, e^5.23, e^7.23, e^9.23, e^{11}.23,$ $e^{13}.23, e^{15}.23, e^{17}.23, e^{19}.23, e^{21}.23, e^{23}.23$

Table 1: The number $Q(2k)$ of quasipolarities in $\mathbb{Z}/2k\mathbb{Z}$ for $1 \leq k \leq 12$, and their explicit enumeration.

Example 3.2. The affine map $e^2.5 : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ is a quasipolarity. Let $p=2$ and $k=\frac{5^2-1}{12}=2$. Since $2 \mid k$, there exists a t such that $5+12t$ is an involution in $\mathbb{Z}/24\mathbb{Z}$. Using the proof of the theorem, t is the solution of

$$0 \equiv 2 \cdot vt \equiv -k \equiv -2 \equiv 0 \pmod 2,$$

thus t can be chosen arbitrarily. If we choose $t = 0$, $k' = \frac{5^2-1}{24} = 1$ is not even. If $t = 1$, then $r = 5 + 12 = 17$ and $k' = \frac{17^2-1}{24} = 12$ is even and $w = pu = 2 \cdot 2 = 4$. Hence $e^4.17 : \mathbb{Z}/24\mathbb{Z} \to \mathbb{Z}/24\mathbb{Z}$ is a quasipolarity such that (4) commutes.

If now we take $p = 5$, we have $5 \nmid 12$, so $t = 3(\pm 1 - 5) \bmod 5 = \pm 3$. If we choose $t = 3$, we get $r = 5 + 2 \cdot 12 = 29$ and it is such that $\frac{r^2-1}{60} = 14$ is even, so $e^{10}.29 : \mathbb{Z}/60\mathbb{Z} \to \mathbb{Z}/60\mathbb{Z}$ satisfies (4).

Acknowledgments

I am very grateful with Prof. Salvatore Giuffrida for his kindness and help regarding the publication of this paper, and I sincerely thank the referee's many observations that improved my exposition and results. I also greatly thank Guerino B. Mazzola and Shalosh B. Ekhad for answering my questions about polarities and quasipolarities with patience and promptness. Last (but surely not least), I thank Frann Grossman at Michigan Technological University for her kind help with the English language.

REFERENCES

[1] O. A. Agustín-Aquino, *Counterpoint in 2k-tone equal temperament*, Journal of Mathematics and Music 3 (3) (2009), 153–164.

[2] O. A. Agustín-Aquino, *Extensiones microtonales de contrapunto*, Ph.D. thesis, Universidad Nacional Autónoma de México, 2011.

[3] O. A. Agustín-Aquino, *Antichains and counterpoint dichotomies*, Contributions to Discrete Mathematics 7 (2) (2012), 97–104.

[4] R. T. Hansen - L. G. Swanson, *Unitary divisors*, Mathematics Magazine 52 (4) (1979), 217–222.

[5] G. Mazzola, *The Topos of Music*, Birkhäuser-Verlag, Basel, 2002.

[6] N. J. A. Sloane, *The On–Line Encyclopedia of Integer Sequences*, A034448.

[7] I. M. Vinogradov, *Elements of number theory*, Dover Publications, Inc., New York, 1954.

OCTAVIO A. AGUSTÍN-AQUINO
Universidad de la Cañada
Carretera Teotitlán-Nanahuatipan S/N
Teotitlán de Flores Magón, Oaxaca
México
e-mail: `octavioalberto@unca.edu.mx`