Pencil of Lines on the 2-D Torus

Raúl Figueroa* and Pablo M. Salzberg†
Department of Mathematics
University of Puerto Rico
P.O. Box 23355, Rio Piedras
Puerto Rico 00931

ABSTRACT. We consider the problem of finding the intersection points of a pencil of lines with rational slope on the 2-dimensional torus. We show that the intersection points belonging to all the lines in the pencil form a finite cyclic group. We also exhibit a generator for this group in terms of the coefficients of the lines. The need for the results presented in this paper arose in dealing with a discrete limited angle model for computerized tomography (Cf. [3], [5]).

1. Preliminary Notations and Definitions

Given (x_1, y_1), $(x_2, y_2) \in R^2$, we denote by E the equivalence relation on R^2 defined by $(x_1, y_1)E(x_2, y_2)$ if and only if $x_2 - x_1$, $y_2 - y_1 \in Z$. The equivalence class of (x, y) is denoted by $[x, y]$. The torus T is defined as the set of all equivalence classes under E, i.e. $T = R^2/E$ or equivalently, $T = R^2/Z^2$. Therefore, $(T, +)$ is an abelian group, where "+" is defined by $[x_1, y_1] + [x_2, y_2] := [x_1 + x_2,\ y_1 + y_2]$. Notice that every equivalence class has a unique representative in the square $[0, 1) \times [0, 1)$, which makes it possible to represent equivalence classes by points in the unit square.

Given $(x, y) \in R^2$, we denote by $\langle [x, y] \rangle$ the subgroup of $(T, +)$ generated by $[x, y]$, i.e., $\langle [x, y] \rangle = \{n[x, y] \mid n \in Z\}$, where $n[x, y] := [nx, ny]$. As usual, the order of an element $[x, y] \in T$ is the least positive integer n such that $n[x, y] = [0, 0]$. Furthermore, if $n, m \in N$, $(n, m) = 1$, and the order of $[x, y]$ is n, then the order of $m[x, y]$ is n, and $\langle m[x, y] \rangle = \langle [x, y] \rangle$. In what follows we shall make use of these results without further reference.

A line on the torus is the subset defined by $\overline{L} = \{[x, y] \in T \mid [x, y] \cap L \neq \emptyset\}$, where L denotes a line on the plane. We define the slope of

*Research supported in part by NSF grants RII-9014056, component IV of the EPSCoR of Puerto Rico Program and ARO grant for Cornell MSI.

†Research supported by the National Institute of Health, MBRS Program, under grant 5S-06GM08102.

$\overline{L}$ as that of L. In what follows we shall consider only lines with rational slope (it is well known that a line with irrational slope is dense on T). Let L_q denote a line on the plane passing through the origin, with rational slope q. From the given definitions it is easy to verify, for $q \in Q$, that $[x, y] \in \overline{L}_q$ if and only if $y + s = q(x + r)$, for some $r, s \in Z$. Moreover, notice that if $[x, y] \in \overline{L}_{q_1} \cap \overline{L}_{q_2}$, where $q_1, q_2 \in Q$ and $q_1 \neq q_2$, then (x, y) satisfies a system of two linear equations in two indeterminates, with rational coefficients. Being unique, the solution of such system is obviously rational. Therefore, $x, y \in Q$.

2. Main Results

In order to state formally our main interest, let $S \subset Q$, where $|S| \geq 2$. As usual, Q denotes the set of rational numbers, and $|X|$ denotes the cardinality of the set X.

Problem: *Find the points in* $J = \bigcap\{\overline{L}_q \mid q \in S\}$.

The information on J will be retrieved by means of some results on finite abelian groups. The reader is referred to Coxeter [1, pp.103–105] and [2], and Schoenberg [6], for applications of similar techniques to the study of certain maps on the torus.

Lemma 1. *Let G be a finite abelian group and let $|G| = p_1^{e_1} \dots p_k^{e_k}$ (p_i prime, $p_i \neq p_j$, $e_i \geq 1$). Then for each p_i, $1 \leq i \leq k$, there is a subgroup $G_{p_i} \subset G$ such that $|G_{p_i}| = p_i^{e_i}$. Furthermore, if G_{p_i} has a unique subgroup of order p_i, then G_{p_i} is cyclic. If each G_{p_i} is cyclic, $1 \leq i \leq k$, then G is cyclic.*

This is a very well known result in group theory and the reader is referred to Suzuki [7] for its proof.

In what follows we shall assume, without any loss in generality, that $(a, b) = 1$ for all $\frac{a}{b} \in S$. Lines of slopes 0 or ∞ will be considered separately.

The following theorem is one of the central results in this paper.

Theorem 1. *$(J, +)$ is a finite cyclic group.*

Proof: *(J is finite.)* Clearly $[0, 0] \in J$, and if $[x_1, y_1]$, $[x_2, y_2] \in J$, then $[x_1, y_1] + [x_2, y_2] \in J$. Therefore J is a subgroup of $(T, +)$. On the other hand, a line L_q with rational slope $q = \frac{n}{d}$ must contain the point (d, n) having integer coordinates. This fact implies that L_q contains $(0, 0)$ and (d, n) which are equivalent under E, and it is clear that if a line on the plane contains two different points equivalent under E, then the representation of the line on the torus will consist of finitely many parallel segments. Therefore, the intersection of any two lines on the torus with different rational slopes must be a finite set, and a-fortiori J must be finite.

(J is cyclic.) If $|J| = 1$, then $J = \{[0,0]\}$ and the proof is concluded. Assume $|J| > 1$ and let $p \mid |J|$, p prime. By Cauchy's theorem, there exists $[x,y] \in J$ of order p. Let us denote $(x,y) = (\frac{r_1}{s_1}, \frac{r_2}{s_2})$, where $r_i, s_i \in Z$ and $(r_i, s_i) = 1$, for $i = 1,2$. Then $[0,0] = p[x,y] = [\frac{r_1 p}{s_1}, \frac{r_2 p}{s_2}]$ implies $\frac{r_i p}{s_i} \in Z$ for $i = 1,2$, which in turn yields $s_1, s_2 \in \{1, p\}$, not both of them being equal to 1. Therefore, every element in J of order p is of one of the following types:

$$\left[\frac{r_1}{p}, 0\right], \left[0, \frac{r_2}{p}\right] \text{ or } \left[\frac{r_1}{p}, \frac{r_2}{p}\right]. \tag{1}$$

Notice that $\langle[\frac{r_1}{p}, 0]\rangle = \langle r_1[\frac{1}{p}, 0]\rangle = \langle[\frac{1}{p}, 0]\rangle$, since $(r_1, p) = 1$. Analogously, $\langle[0, \frac{r_2}{p}]\rangle = \langle[0, \frac{1}{p}]\rangle$ and $\langle[\frac{r_1}{p}, \frac{r_2}{p}]\rangle = \langle[\frac{1}{p}, \frac{r'}{p}]\rangle$ where $(r', p) = 1$. On the other hand, if $[\frac{1}{p}, 0] \in J$, then for each $\frac{a}{b} \in S$, there are $r, s \in Z$ such that $r = \frac{a}{b}(\frac{1}{p} + s)$ which in turn yields $\frac{a}{p} = br - as$. Thus $p \mid a$. Analogously, if $[0, \frac{1}{p}] \in J$, then $p \mid b$ for each $\frac{a}{b} \in S$. Therefore, the subgroups $\langle[\frac{1}{p}, 0]\rangle$ and $\langle[0, \frac{1}{p}]\rangle$ can not coexist in J. Next, assume that $u = [\frac{1}{p}, \frac{r_1}{p}]$ and $v = [\frac{1}{p}, \frac{r_2}{p}]$ belong to J with $\langle u\rangle \neq \langle v\rangle$. Then $r_2 u - r_1 v$ and $u - v$ are of the first and second type of elements given in (1). The fact that both belong to J leads to contradiction.

In general, if J contains any two of the three possible types of elements described in (1), then by performing some elementary arithmetic operations between them it is easy to see that J must contain the three of them, which obviously leads to a contradiction. This shows that J contains a unique subgroup of order p for each prime $p \mid |J|$. From Lemma 1 if follows that J is cyclic, which proves the theorem.

In what follows we shall describe a generator for J in term of the elements of S.

Let $[\frac{\alpha}{\beta}, \frac{\gamma}{\delta}]$ denote a generator for J, i.e.,

$$J = \left\langle \left[\frac{\alpha}{\beta}, \frac{\gamma}{\delta}\right] \right\rangle, \text{ with } (\alpha, \beta) = 1 \text{ and } (\gamma, \delta) = 1. \tag{2}$$

Then $|J| = \text{l.c.m.}(\beta, \delta)$. Indeed, let $u = [\frac{\alpha}{\beta}, 0]$ and $u = [0, \frac{\gamma}{\delta}]$. Clearly, u and v have orders β and δ, respectively. Therefore, $|J| = \text{order } (u + v) = \frac{\beta\delta}{(\beta,\delta)} = \text{l.c.m. } (\beta, \delta)$.

Lemma 2. *Let β, δ be as in (2) and let $\beta' = \frac{\beta}{\mu}$ and $\delta' = \frac{\delta}{\mu}$, where $\mu = g.c.d.\{\beta, \delta\}$. Then the following two assertions hold.*

a) $\beta' = g.c.d.\{c \mid \frac{c}{d} \in S\}$.

b) $\delta' = g.c.d.\{d \mid \frac{c}{d} \in S\}$.

Proof: First, notice that $[\frac{1}{\beta'},0] \in J$ and $[0,\frac{1}{\delta'}] \in J$. Indeed, $(\beta'\gamma,\delta') = 1$ (Cf. (2).) implies the existence of $r,s \in Z$ such that $r\beta'\gamma + s\delta' = 1$, which we rewrite as $r\frac{\beta'\gamma}{\delta'} + s = \frac{1}{\delta'}$. Hence, $r\beta[\frac{\alpha}{\beta},\frac{\gamma}{\delta}] = [0, r\frac{\beta'\gamma}{\delta'}] = [0,\frac{1}{\delta'}] \in J$. The proof for $[\frac{1}{\beta'},0] \in J$ is analogous ($(\beta',\delta'\alpha) = 1$) and will be omitted.

Our next step is to prove that $[\frac{1}{\eta},0] \in J$ if and only if $\eta \mid \beta_1 :=$ g.c.d.$\{c \mid \frac{c}{d} \in S$. For, notice that $[\frac{1}{\eta},0] \in J$ if and only if $[\frac{1}{\eta},0] \in \overline{L}_{c/d}$ for all $\frac{c}{d} \in S$ which, by lemma 1, is equivalent to the existence of integers r,s such that $s = \frac{c}{d}(\frac{1}{\eta} + r)$. This equality is equivalent to $ds - cr = \frac{c}{\eta}$. Finally, under the assumption that $(c,d) = 1$, this last equality holds if and only if $\eta \mid c$, which is true for all integers c for which there exists an integer d such that $\frac{c}{d} \in S$. By taking $\eta = \beta'$ we conclude that $\beta' \mid \beta_1$. On the other hand, given any $[x,0] \in J$ there exists an integer q such that $[x,0] = q[\frac{\alpha}{\beta},\frac{\gamma}{\delta}] = [\frac{q\alpha}{\beta},\frac{q\gamma}{\delta}]$. Therefore $\frac{q}{\delta} \in Z$, i.e., we can write $q = n\delta = n\delta'\mu$, for some $n \in Z$. By replacing q above we obtain $[x,0] = [\frac{n\delta'\alpha}{\beta'},0] = n\delta'\alpha[\frac{1}{\beta'},0]$, i.e., $[x,0] \in \langle[\frac{1}{\beta'},0]\rangle$.

In particular, for $x = \frac{1}{\beta_1}$ we obtain $[\frac{1}{\beta_1},0] \in \langle[\frac{1}{\beta'},0]\rangle$, which implies that $\beta_1 \mid \beta'$ and therefore $\beta_1 = \beta'$.

The proof of part b) follows in a similar form.

Notice that the proof of Lemma 2 implies the following results.

$$\left(\bigcap_{m\in S} \overline{L}_m\right) \cap \overline{L}_0 = \left\langle \left[\frac{1}{\beta'},0\right] \right\rangle, \text{ and} \tag{3}$$

$$\left(\bigcap_{m\in S} \overline{L}_m\right) \cap \overline{L}_\infty = \left\langle \left[0,\frac{1}{\delta'}\right] \right\rangle. \tag{4}$$

Moreover, the intercepts of $\overline{L}_{a/b}$ with the "x-axis" have coordinates $[\frac{i}{a},0]$, for $0 \le i \le |a| - 1$. Analogously, the intercepts of $\overline{L}_{a/b}$ with the "y-axis" have coordinates $[0,\frac{i}{b}]$, for $0 \le i \le |b| - 1$.

We have already characterized β' and δ' in terms of the elements of S. Our next result furnishes a similar characterization for μ, which will allow us to give an explicit expression of a generator for J.

Theorem 2. *Let $\frac{a}{b} \in S$ and denote $a' = \frac{a}{\beta'}$, $b' = \frac{b}{\delta'}$, where β' and δ' were introduced in Lemma 2. Let $\mu_1 =$ g.c.d.$\{a'd' - b'c' \mid \frac{a}{b}, \frac{c}{d} \in S\}$. Then $\mu = \mu_1$ and for any $\frac{a}{b} \in S$, $J = \langle[\frac{b'}{\beta'\mu}, \frac{a'}{\delta'\mu}]\rangle$.*

Proof: Let $\frac{a}{b}$ be an arbitrary but fixed element of S. Then for each $\frac{c}{d} \in S$, there is $n \in Z$ such that $a'd' - b'c' = n\mu_1$. Since $(c,d) = 1$, then $cs - rd = 1$ for some $r,s \in Z$. Therefore, $a'd' - b'c' = n(cs - rd)\mu_1 = (cs' - r'd)\mu_1$, where $s' = ns$ and $r' = nr$. By replacing $d = d'\delta'$ and $c = c'\beta'$ in the right hand side we obtain, after reordering some terms, $d'(a' + r'\delta'\mu_1) = c'(b' + s'\beta'\mu_1)$

which is equivalent to $d(\frac{a'}{\delta'\mu_1} + r') = c(\frac{b'}{\beta'\mu_1} + s')$. These equalities in turn imply that $g = [\frac{b'}{\beta'\mu_1}, \frac{a'}{\delta'\mu_1}] \in J$. It is easy to verify that $(b', \beta'\mu_1) = 1$ and $(a', \delta'\mu_1) = 1$. Therefore, $o(g) = \beta'\delta'\mu_1$ and since $o(g) \mid |J| = \beta'\delta'\mu$ (Cf. comments following (2)), we have that $\mu_1 \mid \mu$.

On the other hand, $g = [\frac{\alpha}{\beta}, \frac{\gamma}{\delta}] \in J$ implies $[\frac{\alpha}{\beta}, \frac{\gamma}{\delta}] \in \overline{L}_{a_i/b_i}$ for any $\frac{a_i}{b_i} \in S$, which in turn yields $\frac{\gamma}{\delta} + r_i = \frac{a_i}{b_i}(\frac{\alpha}{\beta} + s_i)$ for some $r_i, s_i \in Z$. Now, let us consider the system of two such equations obtained for, say, $i = 1, 2$. By taking the difference of the two equations and by clearing denominators we obtain $\beta b_1 b_2(r_1 - r_2) = (a_1 b_2 - b_1 a_2)\alpha + \beta(a_1 b_2 s_1 - a_2 b_1 s_2)$, which after division by $\beta'\delta'$ yields $\mu b'_1 b'_2(r_1 - r_2) = (a'_1 b'_2 - b'_1 a'_2)\alpha + \mu(a_1 b'_2 s_1 - a_2 b'_1 s_2)$. Therefore $\mu \mid a'_1 b'_2 - b'_1 a'_2$ and hence $\mu \mid \mu_1$, which completes the proof.

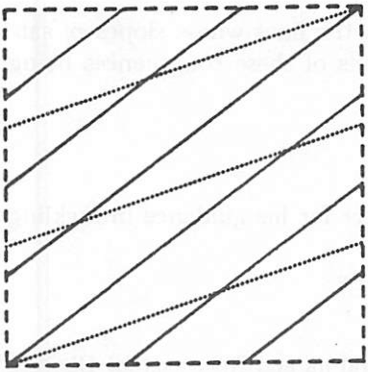

Figure 1.

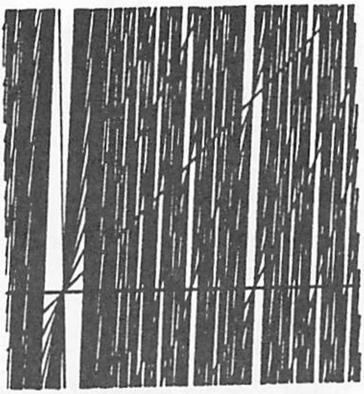

Figure 2.

Example 1: In order to locate the intersection points of the two lines on the torus with slopes $\frac{1}{3}$ and $\frac{3}{4}$ passing through the origin (Cf. Figure 1). We determine $\beta' =$ g.c.d. $\{1, 3\} = 1$, $\delta' =$ g.c.d. $\{3, 4\} = 1$ and $\mu =$ g.c.d. $\{4(1) - 3(3)\} = 5$. Therefore, $J = \langle [\frac{3}{5}, \frac{1}{5}] \rangle = \{(0,0), (\frac{3}{5}, \frac{1}{5}), (\frac{1}{5}, \frac{2}{5}), (\frac{4}{5}, \frac{3}{5}), (\frac{2}{5}, \frac{4}{5})\}$,

Remark: The intersections of all the lines in a pencil passing through an arbitrary point $[x, y]$ in the torus are given by the expression $[x, y] + J = [x + y] + \langle [\frac{b'}{\beta'\mu}, \frac{a'}{\delta'\mu}] \rangle$ (Cf. Theorem 2.)

A particular case of interest in tomography is when the slopes are multiples of a given ratio. An explicit expression is given in the following corollary which extends the main result in [4], and whose proof follows from theorem 2.

Corollary. *Let $q, h \in Z$, $0 \le q < h$ be given, and let $S = \{\frac{c_1}{d}, \frac{c_2}{d}, \dots, \frac{c_k}{d}\}$ be the slopes of a pencil of lines on the torus passing through $[r, s]$, satisfying $c_i \equiv q \pmod{h}$, for $i = 1, \dots, k$. Then $J = \{[r + \frac{i}{h}, s + q\frac{i}{dh} + \frac{j}{d}] \mid 0 \le i \le h, 0 \le j < d\}$.*

Notice that the vertical distance between two consecutive segments (branches) of a line on the torus with slope $\frac{c}{d}$, $(c,d) = 1$, is $\frac{1}{d}$. Hence, given an intersection point of two lines with slopes $\frac{c_1}{d}, \frac{c_2}{d}$, $(c_i, d) = 1$, there will be other $d-1$ equidistant intersection points having the same abscissa as the given point. This fact explains the term $\frac{i}{d}$ in the ordinate of the points of J.

Example 2: The intersections of the pencil of lines given in figure 2 are more difficult to tackle since it includes also the intersections corresponding to sub-pencils. Nevertheless, it is not difficult to prove from that the intersection points of a pen of lines through (r,s) with *integer* slopes $m, 0 \leq m < p$, are given by the expression $[r + \frac{i}{h}, s + q\frac{i}{h}]$, with $0 \leq i$, $q < h < p$ and $(i,h) = 1$.

Moreover, each of these points belongs to the lines whose slopes m satisfy $m \equiv q \pmod{h}$, the number of solutions of these congruences being $[\frac{p-q-1}{h}] + 1$.

Acknowledgment

We are indebted to Professor H.S.M. Coxeter for his guidance in tackling this problem.

References

[1] H.S.M. Coxeter and W.O.J. Moser, "Generators and Relations for Discrete Groups", A Series of Moderns Surveys in Mathematics, 14, Springer-Verlag, 1984.

[2] H.S.M. Coxeter, *The Derivation of Schoenberg's Star-Polytopes from Schoute's Simplex Nets*, in "The Geometric Vein: The Coxeter Festschrift", edited by Ch. Davis, B. Grünbaum and F.A. Sherk, Springer-Verlag, 1981, pp.149–164.

[3] P.M. Salzberg, *Tomography in Projective Spaces: a Heuristic for Limited Angle Reconstructive Models*, SIAM J. Matrix Anal. Appl., **9**, **No. 3**, (1988), pp. 393–398.

[4] P.M. Salzberg, *On the Pattern of Crosses of a Pen of Lines on the 2-D Torus*, Ars Combinatoria, **29-A**, (1990), pp. 107–108.

[5] P.M. Salzberg, *An Applications of Finite Field Theory to Computerized Tomography: A Spatial Limited Angle Model*, Proceedings of the International Conference on Finite Fields, Coding Theory and Advances in Communications and Computing, Marcell Decker, (1992), pp. 395–402.

[6] I.J. Schoenberg, *On the Motion of a Billiard Ball in Two Dimensions*, Delta, **5**, (1975), pp. 1–18.

[7] M. Suzuki, "Group Theory II", Series of Comprehensive Studies in Mathematics, 248, Springer-Verlag, 1985.