The Real Topology of Rational Points on Elliptic Curves

Zachary Scherr

1 Introduction

While reading Andrzej Schinzel's ingenious paper "Triples of positive integers with the same sum and the same product", [1], I came across the following (paraphrased) result

Theorem 1. *Let E be an elliptic curve defined over $\mathbb{Q}$ having rank at least 1. Thinking of $E(\mathbb{R})$ as an embedded manifold in $\mathbb{RP}^2$, then for any rational point $P \in E(\mathbb{Q})$ and any real neighborhood $U \ni P$, one can find infinitely many rational points $P_i \in E(\mathbb{Q})$ such that $P_i \in U$.*

In Schinzel's paper, he needs to prove the existence of infinitely many rational points on an elliptic curve $y^2 = x^3 + Ax + B$ having positive coordinates. He does this by first proving that this curve has rank at least 1, then finding a rational point with positive coordinates, then arguing that there are infinitely many other rational points nearby to this one which must also have positive coordinates.

The reference Shinzel gives to Theorem 1 is the book "Diophantische Gleichungen", by Thoralf Skolem, published in 1950. Since this book is written in German, I decided to work out my own proof of Theorem 1, which will be given here.

2 Proof

When I think about elliptic curves, I tend to think about them as algebro-geometric objects. Theorem 1, however, is really a statement about 1-dimensional real Lie groups. Because of this, first we recall two basic facts from the theory of Lie groups.

Fact 2. *A 1-dimensional, connected, compact Lie group is isomorphic (as Lie groups) to the circle group, S^1.*

Fact 3. *In a Lie group, the connected component of the identity element forms a Lie subgroup.*

With the basic facts in place, we can begin to prove our theorem. First off, we examine what happens if we have an infinite, closed subgroup sitting inside of S^1.

Lemma 4. *Let G be an infinite, closed subgroup of S^1. Then in fact G is all of S^1.*

Proof. Because S^1 is compact, and G is infinite and closed, it must have a limit point $A \in G$. Multiplication by the inverse of A is an isomorphism of Lie groups (in particular it is a homeomorphism), so we see that 1, the identity element of S^1, is also a limit point of G. This means, that for any $\varepsilon > 0$, we can find an element $w = e^{2\pi t} \in G$ with $t < \varepsilon$. Looking at the subgroup that w generates, we see that any arc of S^1 whose length is greater than $2\pi\varepsilon$ must contain a power of w. Thus G is dense in S^1, and since it is closed it must in fact be all of S^1. □

Next, we analyze the topology of a 1-dimensional Lie group.

Proposition 5. *Any compact, 1-dimensional Lie group is homeomorphic to a finite disjoint union of copies of S^1.*

Proof. Let L be a compact, 1-dimensional Lie group. The connected component of L containing the identity element, L_0, is a 1-dimensional, connected, compact Lie subgroup so it is isomorphic to S^1. The group L is a disjoint union of cosets of L_0, and since multiplication is a homeomorphism, each of the cosets of L_0 is topologically homeomorphic to a copy of S^1 (the cosets of L_0 are not subgroups, so they cannot be isomorphic to S^1 as groups). Thus we see that L is homeomorphic to a disjoint union of circles, and since L is compact, it must be a finite disjoint union of circles. □

Remark. For an elliptic curve E defined over the reals, the set of real points of E is isomorphic as a Lie group to either S^1 or $S^1 \times \mathbb{Z}/2\mathbb{Z}$. If we write a model for E as $y^2 = x^3 + Ax + B = f(x)$, the first case occurs when $f(x)$ has one real root, and the second case occurs when $f(x)$ has three real roots.

With everything in place, we are now ready to tackle the structure of infinite, closed subgroups in 1-dimensional, compact Lie groups. The following theorem will give Theorem 1 as a corollary.

Theorem 6. *Let L be a compact, 1-dimensional Lie group. Any infinite, closed subgroup $G \subseteq L$ is also open.*

Proof. Let L_0 denote the identity component of L, and $L_1, \ldots, L_n$ its cosets. Because G is an infinite subset of L, it must intersect at least one of these cosets, L_i, infinitely many times. If $\ell \in L_i \cap G$, then $\ell^{-1} \cdot L_i \cap G$ is contained in $L_0 \cap G$, and has infinite cardinality. Thus the group $G \cap L_0$ is an infinite subgroup of $L_0 \cong S^1$. Because both L_0 and G are closed, their intersection is closed as well, and by Lemma 4, we get that $G \cap L_0 = L_0$. We are now done, because in L_0 there is an open neighborhood $U \ni 1$, the identity element of L. This in turn means that $1 \in U \subseteq L_0 \subseteq G$, and because multiplication is a homeomorphism, we see that G can be written as a union of open sets, $\bigcup_{m \in G} m \cdot U$. □

Corollary 7. *Theorem 1 is true.*

Proof. For the given elliptic curve, E, the set of real points, $E(\mathbb{R})$ is a compact, 1-dimensional Lie group. Because E has rank at least 1, the set of rational points, $E(\mathbb{Q})$, is an infinite subgroup, so its closure, $\overline{E(\mathbb{Q})}$ is an infinite, closed subgroup. By Theorem 6, this group is also open, and hence for any $P \in \overline{E(\mathbb{Q})}$, the full connected component of $E(\mathbb{R})$ containing P must be a subset of $\overline{E(\mathbb{Q})}$. Thus we see that $E(\mathbb{Q})$ is dense in this connected component, and Theorem 1 follows. □

3 Acknowledgements

The author would like to thank his adviser, Michael Zieve, for bringing to his attention the cute paper of Schinzel. The author would also like to thank Julian Rosen for some helpful conversations regarding Lie groups.

4 Bibliography

References

[1] A. Schinzel, *Triples of positive integers with the same sum and the same product*, Serdica Math. J. **22** (1996), no. 4, 587–588. MR **1483607 (98g:**11033)