INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 7 (2007), #A07

A SHORT PROOF OF A KNOWN DENSITY RESULT

Timothy Foo
Department of Mathematics and Computer Science, Rutgers University - Newark, Newark, NJ 07102, USA
tfoo@andromeda.rutgers.edu

Received: 7/26/06, Revised: 1/25/07, Accepted: 1/31/07, Published: 2/3/07

Abstract

A combination of elementary methods and Dirichlet's theorem on the infinitude of primes in arithmetic progressions is used to prove that a certain interesting set is dense in the unit square. The construction of the set involves how an element is related to its multiplicative inverse in the group $(\mathbf{Z}/p\mathbf{Z})^*$.

1. Introduction

The main aim of this paper is to present a short proof of the density of a certain subset of the unit square. The set whose density is proved is the set $\bigcup_p \{(\frac{x}{p}, \frac{y}{p}) : 1 \leq x, y < p,$ and $xy = 1$ mod p$\}$. The results obtained here follow from known results on Kloosterman and hyper-Kloosterman sums. Stronger results can be obtained by using estimates for Kloosterman and hyper-Kloosterman sums. What actually happens (but is not proved here) is the following: Let μ be the normalized Haar measure on the unit square $\mathbf{T}^2$. Let $Y_p = \{(\frac{x}{p}, \frac{y}{p}) : 1 \leq x, y < p, xy = 1 \text{ mod p}\}$. Clearly, $|Y_p| = p - 1$. Let Ω be a domain in $\mathbf{T}^2$ with piecewise smooth boundary. Then $|Y_p \bigcap \Omega| = \mu(\Omega)(p-1) +$ "nice error term". Therefore, if Ω is a circle of radius ϵ, $|Y_p \bigcap \Omega| > 1$ for p sufficiently large. This implies density. See for example [1],[2],[3],[4] and the references therein. It is worth noting that although this proof is short, it uses Dirichlet's theorem on the infinitude of primes in arithmetic progressions.

2. The Construction of the Set

Definition 1 Here, $(\mathbf{Z}/p\mathbf{Z})^*$ will consist of the numbers $1, 2, \ldots, p-1$ rather than the equivalence classes $p\mathbf{Z}+i$. Then $\frac{x}{p}$ is naturally a rational number between 0 and 1 and $(\frac{x}{p}, \frac{y}{p})$ is naturally a point in the unit square with rational coordinates for $x, y \in (\mathbf{Z}/p\mathbf{Z})^*$. By imposing the condition $xy = 1 \pmod p$ for the point $(\frac{x}{p}, \frac{y}{p})$ and taking all such points for a given prime p, one obtains a finite number of points. By taking the union over all primes p

of such a set, one obtains a countable subset of the unit square:

$$A = \bigcup_p \{(\frac{x}{p}, \frac{y}{p}) : xy = 1 \text{ mod p}, \, x, y \in (\mathbf{Z}/p\mathbf{Z})^*\}.$$

Definition 2 We denote the set B by $B = \{(\frac{a}{n}, \frac{n}{b}) : (a, n) = (b, n) = 1, a < n < b\}$.

3. Proof of Density

Lemma 1 The set B is dense in the unit square.

Proof. Take n to be prime to make the proof easier. For fixed n, the x-coordinates $\frac{a}{n}$ are distance $\frac{1}{n}$ apart while the distance between the y-coordinates $\frac{n}{b}$ is bounded by

$$\max(\tfrac{n}{(n+1)(n+2)}, \tfrac{2n}{(2n-1)(2n+1)}).$$

As $n \to \infty$, the distances between the x and y coordinates go to zero. □

Lemma 2 For any point $b \in B$, there exist points in A that are arbitrarily close to b.

Proof. Let $p \equiv -a^{-1}b \pmod n$ and $p \equiv -1 \pmod b$. This is possible due to the Chinese Remainder Theorem. Then $x = \frac{ap+b}{n}$ and $y = \frac{n(p+1)}{b}$ are integers. Furthermore, it is easily verified that $xy \equiv 1 \pmod p$. Then applying Dirichlet's Theorem on the infinitude of primes in arithmetic progressions, there are infinitely many primes satisfying this property. Furthermore, as $p \to \infty$, $\frac{x}{p} \to \frac{a}{n}$ and $\frac{y}{p} \to \frac{n}{b}$. □

From Lemmas 1 and 2 we have the following result.

Theorem 1 A is dense in the unit square.

4. Generalizations to Congruence Classes.

Let $C = u\mathbf{Z}+v$ be any congruence class with infinitely many primes. So $(u, v) = 1$. Theorem 1 can be strengthened as follows.

Theorem 2 The set $\bigcup_{p \in C} \{(\frac{x}{p}, \frac{y}{p}) : xy \equiv 1 \pmod p, \, x, y \in (\mathbf{Z}/p\mathbf{Z})^*\}$ is dense in the unit square.

Proof. Modify the set B to the following set $\{(\frac{a}{n}, \frac{n}{b}) : (a, n) = (b, n) = (u, n) = (u, b) = 1\}$. This set is still dense in the unit square because u is divisible by a finite number of primes. If n is a fixed odd prime not dividing u, the distance between the x-coordinates is still $\frac{1}{n}$ while the distance between the y-coordinates is still bounded by something depending only on n and the number of prime factors of u which is constant. More rigorously, let $L_{u,n} = \{l \in \mathbf{Z} : l > n, (l, n) = (l, u) = 1\}$. Let $a(u, n)$ be the difference between the minimum of $L_{u,n}$ and n. Since u is fixed, we can always find infinitely many primes n so that $n+1 \in L_{u,n}$ which for those n would give $a(u,n) = 1$. Let $r(u,n)$ be the largest possible difference between consecutive numbers in $L_{u,n}$. Then for fixed n, the difference between the y-coordinates in B is bounded by $z(u,n) = \frac{n}{n+a(u,n)} - \frac{n}{n+a(u,n)+r(u,n)}$. As $n \to \infty$, $r(u,n)$ is bounded for fixed u, so $z(u,n) \to 0$. Now, since $p \in C$, the proof of Lemma 2 can be modified by adding the extra condition $p \equiv v \pmod{u}$. The Chinese remainder theorem and Dirichlet's theorem can still be applied. $\square$

5. Generalizations to the Unit Hypercube

It would be interesting to try to generalize this in the following way: Let $f(x_1, x_2, \ldots, x_k) \in \mathbf{Z}[x_1, x_2, \ldots, x_k]$ and consider $\bigcup_p \{(\frac{x_1}{p}, \ldots, \frac{x_k}{p}) : f(x_1, x_2, \ldots, x_k) \equiv 0 \pmod{p}, x_1, x_2, \ldots, x_k \in (\mathbf{Z}/p\mathbf{Z})^*\}$. For what functions f is this dense in the k-dimensional unit hypercube? Here we shall consider $f = \prod_i x_i - 1$ and shall not even prove density but shall mimic the case $f = xy - 1$ to say something about the distribution of points.

Define the following sets:

$A_k = \bigcup_p \{(\frac{x_1}{p}, \frac{x_2}{p}, \ldots, \frac{x_k}{p}) : \prod x_i \equiv 1 \pmod{p}, x_i \in (\mathbf{Z}/p\mathbf{Z})^*\}$;

$B_k = \{(\frac{a_0}{a_1}, \frac{a_1}{a_2}, \ldots, \frac{a_{k-1}}{a_k}) : (a_i, a_j) = 1 \text{ for } i, j > 0, (a_0, a_1) = 1, a_i < a_{i+1}\}$.

Theorem 3 For any point $b \in B_k$, there are points in A_k that are arbitrarily close to b.

Proof. Let $p = -a_0^{-1} a_k \bmod a_1$ and $p = -1 \bmod a_i$ for $i = 2, \ldots, k$. This is possible by the Chinese Remainder Theorem. Let $x_1 = \frac{a_0 p + a_k}{a_1}$, $x_i = \frac{a_{i-1}(p+1)}{a_i}$ for $i = 2, \ldots, k$. Then for all i, $x_i \in \mathbf{Z}$ and $\prod x_i = 1 \pmod{p}$. Then apply Dirichlet's Theorem and let $p \to \infty$. Then $\frac{x_1}{p} \to \frac{a_0}{a_1}$ and $\frac{x_i}{p} \to \frac{a_{i-1}}{a_i}$ for $i = 2, \ldots, k$. $\square$

Acknowledgements I thank Professors Robert Sczech, Jacob Sturm and Zhengyu Mao for very helpful advice. Thanks also to the referee for helpful suggestions and the correction of a typo.

References

[1] M.R. Khan, I.E. Shparlinski, On the maximal difference between an element and its inverse modulo n, Period. Math. Hungar. 47 (2003), no. 1-2, 111–117.

[2] A. Granville, I.E. Shparlinski, A. Zaharescu, On the distribution of rational functions along a curve over F_p and residue races, J. Number Theory 112 (2005), no. 2, 216–237.

[3] K. Ford, M.R. Khan, I.E. Shparlinski, C.L. Yankov, On the maximal difference between an element and its inverse in residue rings, Proc. Amer. Math. Soc. 133 (2005), no. 12, 3463 – 3468.

[4] E. Alkan, F. Stan, A. Zaharescu, Lehmer k−tuples, Proc. Amer. Math. Soc. 134 (2006), no. 10, 2807 – 2815.