TO UNDERSTAND HARDY'S PROOF OF UNIFORM DISTRIBUTION

WILLIAM CHUANG

Contents

1. Introduction.

The main two tools Hardy used are Continued Fraction and the circular dissection method (which is an extension from the Farey's Circle that introduced in Chapter III of [1]). The first question we can ask is why continued fraction is related to rotation of a circle? This will be answered in the section 2.5 (almost everything before section 2.5 is for preparing the foundation for section 2.5). But, to understand the relationship between the two tools, and how to apply them to prove our main theorem (in section 4), it's good know that the main idea of all the following works is to build up a way to approximate irrational by rationals.

- Step 1: To introduce two main tools (continued fraction, and the circular dissection method) which is done in section 2.
- Step 2: Need to show the set S is dense on a circle with unit circumstance which is done in section 3.

Date: March 15, 2018.

- Step 3: Need to show the set S is uniformly distributed[1] which is done in section 4.

where the set $S = \{n\theta | n \in \mathbb{Z}^+, \theta \in \neg\mathbb{Q}\}$. If we don't know the detail of step 2. we still can prove step 3, but since our step 3 is extended the picture of the rotation of circle that was used to prove the claim of step 2. Additionally, if we don't know the difference between S is dense in $(0,1)$ and S is equidistributed in $(0,1)$, it might also be a bit harder to appreciate the proof of equidistribution.

2. Set-up.

2.1. **Some ideas for initiation.**

The initial goal is to build up a way to approximate irrationals by rationals.
Suppose ξ' is given where $\xi' \in \mathbb{R}$. Since what's more interesting is the fractional part, so in the following we rewrite ξ' as ξ, where ξ represents the fraction part of ξ', i.e., $\xi \bmod 1$.
Our goal is to approximate ξ by $r = \frac{p}{q}$ where p and q are integers, $(p,q) = 1$, so r is irreducible. Since the rational are dense in the continuum, there are rationals as near as we wish to any ξ that can eliminate it to approach zero. In other words, given $\xi > 0$, we have

$$\Rightarrow |r - \xi| = \left| \frac{p}{q} - \xi \right| \leq \xi$$

One observation about the possible candidates in an approximation.
$\Rightarrow$Suppose we want to approximate a real number $\alpha = \alpha' \mod 1$ by a rational number $\frac{m}{n}$, and m, n are integers. We can find a number such that $|\frac{m}{n} - \alpha| < \epsilon$, $\forall \epsilon > 0$. But, we may think that's probably not that interesting, because what's really interesting is could we find an n which is sufficiently small but it's still can get a good approximation? We can consider

$$\left\{ \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, ... \frac{n}{n} \right\}$$

as n is sufficiently large, we can get our approximation within the above sequence.

Therefore, we can ask the first question that why continued fraction is used to prove the main theorem? Moreover, this question can be rephrase to a more deeper question:"**The question we can ask is how rapidly can we approximate to** ξ?" Furthermore, this deeper question can be quantified in the following two aspects:

[1] i.e., equidistributed

- Given ξ and $\epsilon > 0$, how complex must $\frac{p}{q}$ be? In other words, how large q must be to secure an approximation with the measure of accuracy ϵ?
- How small can the positive number ϵ be, if we have the upper bound for q?

2.2. **The Starting Point.**

To understand why continued fraction can be used to prove the main theorem, we need to define the so-called "rotation of a circle" or "Farey's circle" first. Then based on this notion, we can extend it to continued fraction that to draw each new level of the approximation of a continued fraction on Farey's circle by using the same algorithm (which is also called the circular method by Hardy).

To define a Farey's circle, we need a notion of Farey's series[2].

2.3. **Farey's Circle.**

Definition. Farey series F_n of order n is the ascending series of irreducible fractions between 0, and 1 whose denominators do not exceed n.
$\Rightarrow \frac{h}{k} \in F_n$ if $0 \leq h \leq k \leq n$, $(h, k) = 1$.

For example,

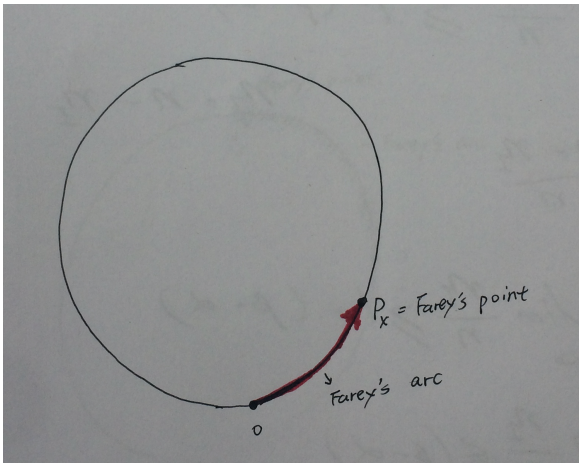
$$F_n = \left\{ \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \right\}.$$

The following are some important properties of **Farey series**:

[2]All the details can be found in CH. III of [1], here I just summarized the necessary results for our purpose.

- If $\frac{h}{k}$ and $\frac{h'}{k'}$ are two successive terms of F_n, then $kh'-hk' = 1$.
  This can be proved by using induction. We just need to suppose it's true for $(n-1)$
- If $\frac{h}{k}$, $\frac{h''}{k''}$, and $\frac{h'}{k'}$ are three successive terms of F_n, then $\frac{h''}{k''} = \frac{h+h'}{k+k'}$.
- In the other way around, if $\frac{h}{k}$, $\frac{h'}{k'}$ are two successive terms of F_n, then the **mediant** $\frac{h+h'}{k+k'}$ of $\frac{h}{k}$ and $\frac{h'}{k'}$ falls in the interval
$$\left(\frac{h}{k}, \frac{h'}{k'}\right)$$

Next, we can consider a circle C of unit circumstance (not a unit circle), and we choose an arbitrary point O of the unit circumference as the representative of 0 (zero). Then we can write any real number x by P_x, in a counter-clockwise orientation. Hence, we can see that O represent all the integers, and the length of the arc form O to P_x is the fraction part after $x - [x]$, i.e. $x]textmod1$. This arc has a name that it's called Farey's arc.



Farey's Dissection

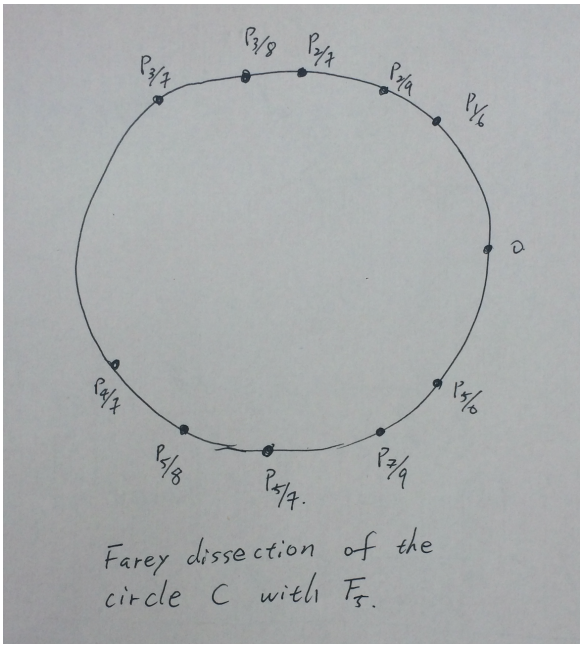
For example, in the above set-up, we already investigate an example as $n = 5$. In F_n, there are ten comma in the sequence, so we know we have ten mediants. We build a new sequence formed by all the mediants of F_5 as follows:

$$M_5 = \left\{\frac{1}{6}, \frac{2}{9}, \frac{2}{7}, \frac{3}{8}, \frac{3}{7}, \frac{4}{7}, \frac{5}{8}, \frac{5}{7}, \frac{7}{9}, \frac{5}{6}\right\}.$$

Therefore, by using GeoGebra, one can draw all the elements in M_5 on C, and call it a Farey's dissection of C. The following is an example:

The property of this M_n sequence are as follows:

- all the mediants in M_n are not in F_n
- the first and last mediants are
$$\frac{1}{n+1}, \frac{n}{n+1}$$
- each point on the circle C is called a Farey point



Therefore, we can derive the *Theorem* ***35*** in Hardy's book:

Theorem 1. *In the Farey dissection of order n, when $n > 1$, each part of the arc which contains the representation of $\frac{h}{k}$ has a length between*
$$\frac{1}{k(2n-1)}, \frac{1}{k(n+1)}.$$

By using Hardy's words: "*The dissection, in fact has a certain uniformity which explains its importance*". Actually, it's an analogue idea of dissection – Banach-Tarski Paradox[3]. Or its less paradoxical problem that the Tarski's circle-squaring problem: **suppose we take a disc in the Euclidean plane, cut it into finitely many pieces, and reassemble all pieces so as to obtain a square with exactly**

[3]A result of selection axiom.

the same area. The idea of solving this problem is the by applying the essence of Euclidean algorithm in a geometrical way to dissect a disc in to finitely many strips. The same essence here, we are thinking about Farey's dissection, but this time we want to be more efficient to approximate an irrational number. And we have a geometrical picture in mind that we want to dissect this circle C (that which has a unit circumstance) by using **the smallest number of steps**.

Furthermore, after we derive the continued fraction (in the next two subsections), we can use it to improve our Theorem **1**, or the Theorem **35** in Hardy's book as follows:
Suppose there exists p, q, where $0 < q \leq n$. From Farey's series, we obtain the following result:

$$\left|\frac{p}{q} - \xi\right| \leq \frac{1}{q(n+1)} < \frac{1}{q^2}.$$

The we multiply both sides by q:

$$|p - \xi q| < \frac{1}{q}$$

which means we divide the circle C into q pieces. After q steps, we can back to the starting point.

2.4. **Farey's Dissection.**
Question: Because of this clue, it leads us to think about Euclidean algorithm–how can we modify this algorithm to give us the most efficient way to find a convergent sequence in this dissection goal?
Answer: *The answer of this question is given by Hardy in Section 10.6 (Page 134[1]). However, the original typesetting is not easy to follow, and it's important to know the derivation so that we can understand why in section 4, we are going to use continued fraction and its result to prove the equidistribution. Therefore, I reconstructed the derivation as following:*

Given any rational fraction $\frac{a_0}{a_1}$, in lowest terms so that $(a_0, a_1) = 1$ and $a_1 > 0$, we apply the Euclidean Algorithm as follows:

$$a_0 = a_1q_0 + a_2, 0 < a_2 < a_1$$
$$a_1 = a_2q_1 + a_3, 0 < a_3 < a_2$$
$$a_2 = a_3q_2 + a_4, 0 < a_4 < a_3$$
$$a_{j-1} = a_jq_{j-1} + a_{j+1}, 0 < a_{j+1} < a_j$$
$$a_j = a_{j+1}q_j$$

Then suppose we let $\lambda_i = \frac{a_i}{a_{i+1}}$ where $0 \leq i \leq j$

$$\Rightarrow \lambda_i = q_i + \frac{1}{\lambda_{i+1}},$$
$$\lambda_j = q_j, 0 \leq i \leq j-1.$$

Hence suppose we take the first two of these equations, those for which $i = 0$, and $i = 1$, and eliminate λ_1, so we obtain

$$\lambda_0 = q_0 + \frac{1}{q_1 + \frac{1}{\lambda_2}}$$

Likewise, we can replace λ_2, and λ_3....

In summary, we just derived the continued fraction from Euclidean Algorithm, and it's due to the property of Euclidean Algorithm, we know that this is the most efficient way to do the circular method of dissection:

$$\lambda_0 = \frac{q_0}{q_1} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \ldots + \frac{1}{\left(q_{j-1} + \frac{1}{q_j}\right)}}}.$$

In our purpose, for λ_0 our goal is to do the most efficient circular dissection, so we only need to focus on the fractional part:

$$\lambda_0 \ \mathbf{mod}\ 1 = \frac{1}{\lambda_1}$$

Hence, the first point on the circle C can be denoted as $p_1 = \frac{1}{\lambda_1}$. Furthermore, this fraction equally divided the circle C which has a unit circumstance into λ_1 pieces. Also, after λ_1 we can back to the starting point.

For the second level of precision, we consider to use λ_2:

$$\lambda_0 \ \mathbf{mod}\ 1 = \frac{1}{\lambda_1} = \frac{1}{q_1 + \frac{1}{\lambda_2}} = q_0 + \frac{\lambda_2}{q_1\lambda_2 + 1}$$

Hence, the first point on the circle C can be denoted as $p_2 = \frac{\lambda_2}{\lambda_2 q_2 + 1}$. Furthermore, this fraction equally divided the circle C which has a unit circumstance into $\lambda_2 q_2 + 1$ pieces. Also, the worst case is $(\lambda_2, \lambda_2 q_2 + 1) = 1$, so even this is the case, we are sure that after $\lambda_2 \cdot (\lambda_2 q_2 + 1)$ steps, we can back to the starting point.

Likewise, in the third level, we have:

$$\lambda_0 \ \mathbf{mod}\ 1 = \frac{1}{\lambda_1} = \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\lambda_3}}} = q_0 + \frac{1 + \lambda_3 q_2}{\lambda_3 q_1 q_2 + q_1 + \lambda_3}$$

It follows that, the first point on the circle C can be denoted as $p_3 = \frac{\lambda_3 q_2 + 1}{\lambda_3 q_1 q_2 + q_1 + \lambda_3}$. Furthermore, this fraction equally divided the circle C which has a unit circumstance into $\lambda_2 q_2 + 1$ pieces. Also, the worst case is $(\lambda_2 q_2 + 1, \lambda_3 q_1 q_2 + q_1 + \lambda_3) = 1$, so even this is the case, we are sure that after $(\lambda_2 q_2 + 1) \cdot (\lambda_3 q_1 q_2 + q_1 + \lambda_3)$ steps, we can back to the starting point.

2.5. **Continued Fraction Expansion.**
The following is a well-known result which is one of the most important direct result of continued fraction that can help us to improve the result in the previous section.

Fundamental Recurrence Relation

Theorem 2. *Let p_n and q_n be the convergents. Then*

$$\det\left(\begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}\right) = p_n q_{n-1} - p_{n-1}q_n = (-1)^n, \text{ for all } n \geq 0.$$

Proof. We can prove this statement by mathematical induction. First of all, we check the base case, as $n = 0$, and $n = 1$:

$$p_0 q_{-1} - p_{-1}q_0 = 1(1) - 0(0) = 1 = (-1)^0$$

which is okay.
For $n = 1$, we obtain:

$$p_1 q_0 - p_0 q_1 = (a_1 p_0 + p_{-1})(0) - 1(a_1 q_0 + q_1)$$

$$= 0 - 1(0 + 1) = -1 = -(1)^1.$$

Both case are valid.
Thirdly, we assume it holds for all $n \leq k$, so we nee to show this is true as $n = k + 1$.

$$\begin{aligned} p_{k+1}q_k - p_k q_{k+1} &= (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1}) \\ &= a_{k+1}p_k q_k + p_{k-1}q_k - a_{k+1}p_k q_k - p_k q_{k-1} \\ &= p_{k-1}q_k - p_k q_{k-1} \\ &= -(p_k q_{k-1} - p_k - 1q_k) \\ &= -(-1)^k \\ &= (-1)^{k+1}. \end{aligned}$$

This completes the proof. □

Now, we divide both sides by $q_n \cdot q_{n-1}$, let $x = \frac{p_{n-1}}{q_{n-1}}$. Then we can know that we have found a smaller bound by using continued fraction, compared to Dirichlet Theorem[4].

[4]A proof is attached in the appendix for self-contained reason

Continued Fraction Expansion

This method converges in a running time of order $\log n$ (the last section of our proof is an example for showing this time complexity):

$$\left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_{n-1} q_n}.$$

3. To prove S is dense on C

According to Hardy's book[1], Dirichlet's Theorem **201** states that: Given any set of real numbers $\theta_1, \theta_2, \theta_3, ...\theta_k$, we can make $n\theta_1, n\theta_2, ..., n\theta_k$ all differs from integers by as small as possible. ($\theta_k, k \in \mathbb{Z}$ is a fraction of an irrational number)

Suppose we are given two numbers θ and α, the question we can ask is: Can we find an integer n to make $n\theta - \alpha$ is nearly an integer? If θ is a rational number, and $\theta = \frac{a}{b}$, where a, b are integers, and $\frac{a}{b}$ is irreducible, then

$$(n\theta) = n\theta - [n\theta]$$
$$(n\theta) \in K = \left\{ \frac{0}{b}, \frac{1}{b}, \frac{2}{b}, ..., \frac{b-1}{b} \right\}$$

and we need to think these points are evenly divided the circle C (a circle with unit circumstance as in previous section).
Hence, if $0 < \alpha < 1$, and α is not one of elements of K, then

$$\left| \frac{r}{b} - \alpha \right|, r = 0, 1, 2, 3, ..., b$$

has a positive minimum μ, i.e.,

$$\mu = min \left\{ \left| \frac{r}{b} - \alpha \right|, r = 0, 1, 2, 3, ..., b \right\}$$

and $n\theta - \alpha$ (θ is an irrational number, but we can think it as a fraction part of an irrational number due to the following reason) cannot differ from an integer less than μ. Since all points are on C, this representation automatically rejects integers; in other words, 0 and 1 are represented by the same point of the circle, thus in general $n\theta = (n\theta)$.

Next, we need to show:

Theorem 3. $(n\theta)$ ***is dense in*** C, *i.e.,* $(0,1)$ *where* $n = 1, 2, 3, ...,$ *and* θ *is an irrational number.*

- *There is no* $n\theta$ *pint can fall at* 0*, and no two of* $n\theta$ *points coincide on the circle* C*.*
- *As introduced in the abstract, the set* S *is collecting all* $n\theta$*, and has a derived set* S'*.*

Proof. To say S is dense on the circle C is to say every α belongs to the derived set S'. If $\alpha \in S$, but $\alpha \notin S$, there is an interval $I_1 = (\alpha - t, \alpha + t)$, $t \in \mathbb{R}$. Then $\forall x \in I_1$, $x \notin S$, if $x \neq \alpha$, then $\exists x \in I_1, x \notin S, x \notin S'$, if $x \neq \alpha$. Hence, to prove the theorem, it is sufficient to prove that every $\alpha \in S$, or $\alpha \notin S'$. And, we are going to prove this by contradiction.
If not, $\exists I_i = (\alpha - \delta, \alpha + \delta'), \delta > 0, \delta' > 0$ where $\forall x \in I_i$, $x \notin S$. We denote the greatest interval among all I_i.

Hence, if α has $I(\alpha)$ (that $\forall x \in I(\alpha), x \notin S$)
then $\alpha - \theta$ has $I(\alpha)$
$\alpha - 2\theta$ has $I(\alpha - 2\theta)$
$\alpha - 3\theta$ has $I(\alpha - 3\theta)$
.....
$\alpha - n\theta$ has $I(\alpha - n\theta)$.
However, we are on a circle and no two of these intervals $(I(\alpha - n\theta))$ can coincide (since $\theta \in \neg Q$), and no two of these intervals can overlap, since overlapping of two intervals constitute together a larger interval. But, the length of circumstance of C is finite, so it cannot contain infinitely many of $I(\alpha - n\theta)$. This contradiction shows that there can be no interval $I(\alpha)$. Thus, we have proven that $\alpha \in S$ or $\alpha \in S'$, and so S is dense on the circle C, i.e., in $(0,1)$. □

4. To prove S is equidistributed on C

The idea of defining the terminology: "equidistribution." A set of points P_n in $(0,1)$ is uniformly distributed if every subinterval of $(0,1)$ contains its appropriate amount of points. The following is a formal (quantified) definition:

Definition. Suppose $I = (\alpha, \beta)$, β, and $\alpha \in \mathbb{R}^a$. If $n_I =$ # of points P_i which fall in I and $\frac{n_I}{n} \to \beta - \alpha$ whatever I when $n \to \infty$, then the set is equidistributed.

[a]Hardy denotes I both for the interval and its length (e.g. $I = (0, I)$), but I decided to use $(\alpha - \beta)$ to denote the length of the interval $I = (\alpha, \beta), \alpha, \beta \in \mathbb{R}$ instead. This is especially important in this section when we start to prove the main theorem of this essay.

The following is the main theorem of this essay that we need to prove:

Theorem 4. *If θ is irrational, then the points $(n\theta)$ are uniformly distributed in $(0, 1)$.*

The following proof is based on the tools we developed in the previous sections: Continued fraction, and circular method (and the what we did in Step 2 can also be seen as an simpler example of the use of circular method).

Proof. **It's extremely important to always keep in mind for doing the following argument that M is not only positive, but also an integer, and so as all the numerators: $c, d, M,$ and w. (Again, they're all positive integers.)**

Suppose we choose an integer $M > 0$[5] to be the *inverse* smallest scale on the circle C (a circle with unit circumstance)[6]. We let the value of this scale is quantified by a positive real number ϵ in a way that

$$\frac{1}{M} < \frac{1}{2}\epsilon < \frac{1}{2},$$

the one-half means we at most consider the largest step of the circular method should be less than a half of the length of the circumstance of C, i.e., $(0, 1)$. Or, in other words, due to the inequality, we at least can have three steps to back to the starting point O.

Suppose a_v is the denominator of one of the convergent of θ.

[5]It's extremely important to remember that M is not only positive, but also an integer, and so as all the numerators: c, d, M, and w.

[6]In other words, if we take the inverse of M, then it tells us how many evenly small pieces of the length of the circumstance of the circle C we can get.

To assemble the notion of continued fraction into this proof, we impose one more constraint on this smallest scale on the circle C by assuming that we have

$$a_v \leq \frac{n}{M} < a_{v+1} \tag{1}$$

Now, we assume the scale is fixed, so M is fixed. We take $n \to \infty$, then by equation (1), we know that $v \to \infty$. It follows that according to our derivation in section 2.4, the v-th level convergent of a continued fraction of θ is a_v, and $a_v \to \infty$, and so as $a_{v+1} \to \infty$. Also, by multiplying the inverse smallest scale M with a coefficient 3 we obtain:

$$3M\left(\frac{1}{a_v}\right) < \frac{1}{2} \tag{2}$$

This mysterious factor 3 will be useful in the inequality (16).
Next, let r be the positive integer, and we divide n in the following way:

$$n = ra_v + s, 0 \leq s < a_v, \tag{3}$$

it follows

$$\frac{n}{a_v} = \left(r + \frac{s}{a_v}\right) < (r+1) \tag{4}$$

which gives

$$M \leq \frac{n}{a_v} = \left(r + \frac{s}{a_v}\right) < (r+1) \tag{5}$$

and

$$M < (r+1). \tag{6}$$

Furthermore,

$$M \leq r \leq \frac{n}{a_v}. \tag{7}$$

The next thing we need to do is to take two fractional part of two real number and called them α, and β, and $\alpha < \beta$. Then, we can get an interval $I = (\alpha, \beta)$. Then, let's use three more restrictions to constraints this interval as follows.

Next, we choose two integers c and d, such that $c < d$, and this implies

$$\frac{c}{a_v} < \frac{d}{a_v}. \tag{8}$$

One must also assume that $\alpha \leq c < d \leq \beta$, thus

$$\alpha \leq \frac{c}{a_v} < \frac{d}{a_v}\beta. \tag{9}$$

Now, we impose the third constraint:

$$\frac{c-1}{a_v} \leq \alpha \leq \frac{c}{a_v}$$

and

$$\frac{d}{a_v} \leq \beta < \frac{d+1}{a_v}.$$

Therefore, we derive the following inequalities:

$$\frac{c-1}{a_v} \leq \alpha \leq \frac{c}{a_v} < \frac{d}{a_v} \leq \beta < \frac{d+1}{a_v} \tag{10}$$

If take $n \to \infty$ (we already knew then $v \to \infty$, and the denominator of v-th level of the continued fraction of θ also goes to infinity, and $a_v \to \infty$), then $(d-c) \to \infty$.

The next important step is to consider points of

$$\frac{w}{a_v},$$

w is an integer. Furthermore, we impose a constraint on points of $\frac{w}{a_v}$ in the following inequalities:

$$c + M \leq w \leq d - M.$$

Therefore,

$$\left(\frac{c}{a_v} + \frac{M}{a_v}\right) \leq \frac{w}{a_v} \leq \left(\frac{d}{a_v} - \frac{M}{a_v}\right) \tag{11}$$

and we can do a bit more on this:

$$\alpha \leq \frac{c}{a_v} < \frac{c}{a_v} + \frac{M}{a_v} \leq \frac{w}{a_v} \leq \frac{d}{a_v} - \frac{M}{a_v} < \frac{d}{a_v} \leq \beta \tag{12}$$

and then we can go even further to make the above inequalities more longer:

$$\frac{c-1}{a_v} < \alpha \leq \frac{c}{a_v} < \frac{c}{a_v} + \frac{M}{a_v} \leq \frac{w}{a_v} \leq \frac{d}{a_v} - \frac{M}{a_v} < \frac{d}{a_v} \leq \beta < \frac{d+1}{a_v} \tag{13}$$

and finally the complete form (all the numbers are points drew on the unit circumstance of circle C):

$$0 = \frac{0}{a_v} \leq \frac{c-1}{a_v} < \alpha \leq \frac{c}{a_v} < \frac{c}{a_v} + \frac{M}{a_v} \leq \frac{w}{a_v} \leq \frac{d}{a_v} - \frac{M}{a_v} < \frac{d}{a_v} \leq \beta < \frac{d+1}{a_v} \leq \frac{a_v - 1}{a_v} \tag{14}$$

Now, let's denote the interval

$$I' = \left(\alpha + \frac{M}{a_v}, \beta - \frac{M}{a_v}\right). \tag{15}$$

If a point $P' \in I$, and the Euclidean distance $d(P', P) < \frac{M}{a_v}$, then for sure $P \in I = (\alpha, \beta)$.

Next, recall the $n\theta$ in the claim of the main theorem, here let's take the following points where $(n \geq m)$

$$m\theta_v = m\frac{b_v}{a_v}$$

where m, b_v, a_v are integers, and θ_v is the v-th convergent of the continued fraction of θ.
Now, once all of these points are drawn on the circle C, for sure they will coincide with $\frac{w}{a_v}$, since it goes to infinity, and always mod 1. But, here what's more interesting is to look at the first a_v number of these points. And they form a set as follows:

$$K = \left\{\frac{0}{a_v}, \frac{1}{a_v}, \frac{2}{a_v}, ..., \frac{a_v - 1}{a_v}.\right\}$$

Also, please remember that all of these elements of the set K are drawn like we did for Farey's points on the circle C.
I also knew the number

$$m\frac{b_v}{a_v}(\text{ mod } 1) \in \left\{\frac{0}{a_v}, \frac{1}{a_v}, ..., \frac{a_v-1}{a_v}\right\} := K'.$$

Moreover, we also knew the number of $m\frac{b_v}{a_v}$ in K' is $N := d-c-2M+1$[7], i.e., there are N many of $m\frac{b_v}{a_v}$ mod 1 points lie in the interval I'.

In other words, there are N many $\frac{w}{a_v}$ points lie in the interval $I' = \left(\alpha + \frac{M}{a_v}, \beta - \frac{M}{a_v}\right)$.
Since we have already known

$$\frac{n}{a_v} \geq r,$$

hence we also can know

$$n \geq ra_v.$$

Also, for sure from (14), we can see that it's obvious that $a_n \geq N = d-c-2M+1$, so we have

$$n \geq ra_v \geq rN.$$

Therefore, there are at least rN many of the first n points of $m\frac{b_v}{a_v}$ are located in I'.

Since

$$\frac{c-1}{a_v} < \alpha < \beta < \frac{d+1}{a_v},$$

thus

$$|\beta - \alpha| = \beta - \alpha < \frac{d-c+2}{a_v}$$

and hence

$$\Rightarrow r\cdot N > r\cdot(a_v\cdot(\beta-\alpha)-2M-1) \geq r\cdot(a_v\cdot(\beta-\alpha)-2M-M) = r\cdot(a_v\cdot(\beta-\alpha)-3M)$$

(the last inequality is due to $M > 0$, and as I reminded in the first line of this proof that M is an integer.)

It follows that

$$rN > r\cdot(a_v\cdot(\beta-\alpha)-3M) = (n-s)(\beta-\alpha)-3Mr. \tag{16}$$

[7]Here we can see the advantage to make all the numerators to be integers, because we can easily count the number of points between two bounds.

Because we also know that in equation (3) we have $0 \leq s < a_r$, so we can write down the following inequalities:

$$s(\beta - \alpha) \leq s < sa_v \leq \frac{n}{M} < \frac{1}{2}\epsilon \cdot n \tag{17}$$

On the other hand, we have $r \leq \frac{n}{a_v}$, so we can derive:

$$3Mr \leq \frac{3Mr}{a_v} < \frac{1}{2}\epsilon \cdot n. \tag{18}$$

Plug inequalities (17) and (18) into (16):

(19)

$$rN > \big((n-s)(\beta-\alpha) - 3Mr\big) = \big(n(\beta-\alpha) - s(\beta-\alpha) - 3Mr\big) > n(\beta-\alpha) - \frac{1}{2}\epsilon n - \frac{1}{2}\epsilon n.$$

That is

$$rN > n\left((\beta-\alpha) - \epsilon\right), N := d - c - 2M + 1. \tag{20}$$

where $n \geq m$, and we are especially interested the case when n is sufficiently large.

Now, finally we can apply the result we derived in section 2.5 (the continued fraction expansion form fundamental recurrence relation). Since from section 2.5, we have:

$$|\theta - \theta_v| < \frac{1}{q_v q_{v+1}} < \frac{1}{q_v^2}.$$

From (1), We also knew that

$$\frac{n}{a_v} \geq M.$$

Therefore,

$$\Rightarrow |m\theta - m\theta_v| \leq |n\theta - n\theta_v| < \frac{n}{q_v q_{v+1}} < \frac{M}{a_v}$$

Now, recall the boxed result of $P \in I = (\alpha, \beta)$, and equation (15):

since $m\theta_v \in I'$ and

$$d(P, P_v) = d(m\theta, m\theta_v) < \frac{M}{q_v}, \tag{21}$$

hence

$$P = m\theta \in I.$$

Denote $N' :=$ the number of $P = m\theta \in I$ where $n \geq m$.

Please recall that $rN :=$ the first n points of $m\frac{b_v}{a_v} \in I' =$ the number of $P_v = m\theta_v = \frac{w}{a_v} \in I'$ and $rN > n((\beta - \alpha) - \epsilon)$.

Then, because we already knew the number of points of P_v in I' is the number of points of $m\theta_v = \frac{w}{a_v} = rN > n((\beta - \alpha) - \epsilon)$, and now we have (21), so by (15) we know the number of $P = m\theta \in I$, like P_v, must also be at least greater than $n((\beta - \alpha) - \epsilon)$.

$$rN > n((\beta - \alpha) - \epsilon) \Rightarrow N' > n((\beta - \alpha) - \epsilon)$$

$$\Rightarrow \lim_{n\to\infty} \inf \frac{n_I}{n} > (\beta - \alpha) - \epsilon$$

where $n_I =$ all the points in the interval I. Since ϵ is arbitrarily chosen, so it can be chosen arbitrarily small. Hence,

$$\Rightarrow \lim_{n\to\infty} \inf \frac{n_I}{n} \geq (\beta - \alpha).$$

Likewise, if we denote J as the complement of interval I on the circle C (a circle with unit circumstance that we used to put all the points on it), i.e., J has a length $1 - (\beta - \alpha)$. Then, with the same procedure as above, we derive the other direction that:

$$\Rightarrow \lim_{n\to\infty} \sup \frac{n_J}{n} \geq 1 - (\beta - \alpha),$$

where $n_J := n - n_I$.
Thus,

$$\Rightarrow \lim_{n\to\infty} \sup \frac{n - n_I}{n} = 1 - \lim_{n\to\infty} \sup \frac{n_I}{n} \geq 1 - (\beta - \alpha),$$

$$\Rightarrow \lim_{n\to\infty} \sup \frac{n_I}{n} \leq (\beta - \alpha).$$

Hence, we have both

$$\lim_{n\to\infty} \sup \frac{n_I}{n} \leq (\beta - \alpha),$$

and

$$\lim_{n\to\infty} \inf \frac{n_I}{n} \geq (\beta - \alpha),$$

It follows that

$$\frac{n_I}{n} \to (\beta - \alpha),$$

then by definition, this completes the proof.

□

5. References.

[1] G. Hardy and E. Wright, Introduction to the Theory of Numbers, 4th Edition, Oxford, 1975.

6. Appendix.

6.1. **Dirichlet Theorem.**

To prove Dirichlet Theorem, we need the following definition.

Denote $\lfloor x \rfloor$ as the integral part of a real number x, and $(x) := x - \lfloor x \rfloor$ as the fractional part of x.

Dirichlet Theorem

Theorem 5. *Let $\xi' \in \mathbb{R}$ be given. If ξ' is real, then there exists rational numbers p, and q, and $(p, q) = 1$, such that $\left|\xi' - \frac{p}{q}\right| \leq \frac{1}{q^2}$.*

Proof. Let $\xi = (\xi')$. Let $m > 1$ be a fixed integer. Consider the following $m+1$ elements in a sequence: 0, (ξ), (2ξ), (3ξ), (4ξ), ..., $(m\xi)$. Secondly, consider m intervals: $\left[\frac{i}{m}, \frac{i+1}{m}\right)$ where $i \in \{0, 1, 2, ..., m-1\}$.

By the pigeon hole principle, since we have $m+1$ elements, but only m intervals, hence some two fractional parts fall into the same interval, $a\xi$ and $b\xi$ with $0 \leq a < b \leq m$, and that interval let's denote it as $\left[\frac{j}{m}, \frac{j+1}{m}\right)$.

Recall a fact that suppose $x \in \mathbb{R}$, and $y \in \mathbb{R}$, then $\exists n \in \mathbb{Z}$ such that $|x - y| = n + d$, where $d = |(x) - (y)|$. Here, we let $n = p$, $x = a\xi$, and $y = b\xi$.

Then by using this fact we can estimate the distance from the number $|x - y|$ to some integer p as follows:

$$||x - y| - p| = |\,|a - b| \cdot \xi - p| = |d| < \frac{1}{m}.$$

That is $|a - b| \cdot \xi$ is less that $\frac{1}{m}$ distant from some integer p.

***Notice that** $|a - b|$ **is a positive integer not greater than** m**.** Let's choose it to be q, then we just found that

$$|\,|a - b| \cdot \xi - p| = |q\xi - p| < \frac{1}{m}$$

$$\Rightarrow |q\xi - p| < \frac{1}{m} \leq \frac{1}{q}.$$

Then once we divide both sides by q***, this completes the theorem.***

□

Remark. Additionally, if ξ is irrational, then there exist an infinite sequence $\frac{p_n}{q_n}$. To see this, consider that thus far, we have found one such q. However, why can we claim it's infinitely many? It follows from an observation that this proof actually can be seen as an algorithm that generates a $q \in [1, m]$ such that $|q\xi - p| < \frac{1}{m}$.