A LEMMA FOR B-R-C THEOREM

JAEIK CHOI

Abstract. Bruck-Ryser-Chowla theorem implies a corollary related to the criterion for non-existence of π_q. To prove this theorem, we first need to prove lemmas. One of them is as follows: for some $n \in \mathbb{N}$ and $x, y, z \in \mathbb{Z}$, we have $x^2 + y^2 = nz^2$ if and only if $n = a^2 + b^2$ for $a, b \in \mathbb{N}$. We will first look at the pigeonhole property necessary to prove this lemma and we will provide the proof of the lemma using this property.

1. Introduction

A incidence structure $\pi = (\mathcal{P}, \mathcal{L})$ is called projective plane if it satisfies the following properties;
(1) $\forall\, P, Q \in \mathcal{P}$, $\exists!\, \ell \in \mathcal{L}$ with $P, Q \in \ell$
(2) $\forall\, \ell, m \in \mathcal{L}$, $\exists!\, P \in \mathcal{P}$ with $P \in \ell \cap m$
(3) $\exists$ four points in π such that none of three are linear.

Lemma 1.1. *For a finite projective plane π, there is $q \in \mathbb{N}$ such that*
(1) $|\ell| = q + 1$ for each $\ell \in \mathcal{L}$;
(2) $|\ell(P)| = q + 1$ for each $P \in \mathcal{P}$.

We use a notation π_q to denote the projective plane of order q. It is an important to know the existence of π_q. We know that Bruck-Ryser-Chowla theorem implies a corollary related to the criterion for non-existence of π_q. To prove the B-R-C theorem, the following lemma is required.

Lemma 1.2. *For some $n \in \mathbb{N} \cup \{0\}$ and $x, y, z \in \mathbb{Z}$, we have $x^2 + y^2 = nz^2$ if and only if $n = a^2 + b^2$ for $a, b \in \mathbb{N} \cup \{0\}$. ($x, y$ and z not all are 0.)*

We will first look at the pigeonhole property which is used to prove this lemma and we will provide the complete proof of the lemma using this property.

2. pigeonhole property

The pigeonhole property is the following statement.

Theorem 2.1 (Pigeonhole property)**.** *If n items are put into m containers, with $n > m$, then at least one container must contain more than one item.*

Key words and phrases. a lemma for B-R-C theorem, the pigeonhole property.

It is said that the pigeonhole property was invented by Jean Leurechon (c. 1591 – 1670) who is the French mathematician. Although the pigeonhole property appears as early as 1624 in a book attributed to Jean Leurechon, it is commonly called Dirichlet's box principle or Dirichlet's drawer principle after an 1834 treatment of the principle by Peter Gustav Lejeune Dirichlet.


FIGURE 1. Jean Leurechon, Peter Gustav Lejeune Dirichlet

Proof. Suppose that there exist $n+1$ items and n containers. Assume that each container contains no more than one item. Then there are at most n items in the containers. This is a Contradiction. Thus, at least one container must contain more than one item. □

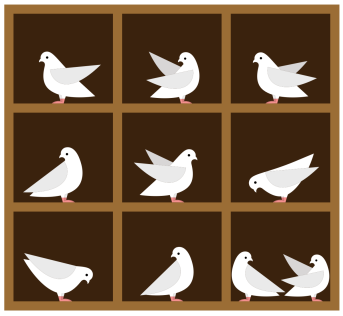

FIGURE 2. 10 pigeons and 9 pigeonholes

Here is an example. Suppose that there exists 10 pigeons and 9 pigeonholes. In order for all pigeons to enter the nest, at least two must enter one nest. This property is very simple, but powerful.

3. The B-R-C theorem

The B-R-C theorem is as follows.

Theorem 3.1 (Bruck-Ryser-Chowla)**.** *Let $(P, \mathcal{B}, \mathcal{I})$ be a (v, b, r, k, λ) BIBD.*
(1) If there exists a symmetric (v, b, r, k, λ) BIBD for even v, then $k - \lambda$ is a perfect square.
(2) If there exists a symmetric (v, b, r, k, λ) BIBD for odd v, then there is a set of integral solution x, y, and z (not all are 0) of the Diophantine equation $x^2 = (k - \lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda z^2$.

Corollary 3.2. *If $q \neq a^2 + b^2$ and $q \equiv 1, 2 \ (mod\, 4)$, then π_q does not exist.*

For example, we know that 6 cannot be expressed as the sum of two square numbers and $6 \equiv 2 \ (mod\, 4)$. Thus, there is no projective plane of order 6.

4. proof of the lemma for B-R-C theorem

To prove the lemma for B-R-C theorem, we need the following lemma.

Lemma 4.1. *Let $x^2 + y^2 = nz^2$ for some $n \in \mathbb{N} \cup \{0\}$ and $x, y, z \in \mathbb{Z}$. Then $gcd(x, y) = 1$ implies $gcd(x, n) = 1$.*

Proof. We prove this lemma by contraposition. Suppose that $gcd(x, n) = d > 1$. Then $d \,|\, y^2$. There exists a prime such that $p \,|\, d$ since $d > 1$. This implies that $p \,|\, y$. Thus, $\gcd(x, y) \geq p > 1$. □

Now we are ready to prove the lemma for B-R-C theorem.

Lemma 4.2. *For some $n \in \mathbb{N} \cup \{0\}$ and $x, y, z \in \mathbb{Z}$, we have $x^2 + y^2 = nz^2$ if and only if $n = a^2 + b^2$ for $a, b \in \mathbb{N} \cup \{0\}$. ($x, y$ and z not all are 0.)*

Proof ($\Leftarrow$). Suppose that $n = a^2 + b^2$ for some $a, b \in \mathbb{N} \cup \{0\}$. Then we get the equation $nz^2 = (az)^2 + (bz)^2$ where $z \in \mathbb{Z}$. Let $x = az$, $y = bz$. Then $nz^2 = x^2 + y^2$ and $n \in \mathbb{N} \cup \{0\}, x \in \mathbb{Z}$ and $y \in \mathbb{Z}$.

($\Rightarrow$). Suppose that $x^2 + y^2 = nz^2$ for some $n \in \mathbb{N} \cup \{0\}$ and $x, y, z \in \mathbb{Z}$. It is sufficient to prove this under the case that $gcd(x, y) = 1$. (We will explain later.) Suppose that n is not a square. There uniquely exists $t \in \mathbb{N}$ such that $t^2 < n < (t+1)^2$. Suppose that there exist $(t+1)^2$ distinct integer of the form $xu + yv$ with $0 \leq u, v \leq t$. (If not, we can skip the step of using the pigeonhole property.) By the pigeonhole property, there exist $(u, v), (u', v')$ such that $(xu + yv) \equiv k \equiv (xu' + yv') \pmod{n}$ for some $0 \leq k < n$. This implies $x(u - u') + y(v - v') \equiv 0 \pmod{n}$. Let $a = u - u', b = v - v'$. Then we get $0 < a^2 + b^2 < 2n$ since $|a|, |b| \leq t$. The equation $xa + yb \equiv 0 \pmod{n}$ implies that $x^2a^2 - y^2b^2 \equiv 0 \pmod{n}$. Also, we get the equation $x^2b^2 + y^2b^2 \equiv 0 \pmod{n}$ from $x^2 + y^2 = nz^2$. The sum of two equiation implies that $n \,|\, x^2(a^2 + b^2)$. By the **lemma 4.1**, We get $n \,|\, (a^2 + b^2)$. Therefore, we get $n = a^2 + b^2$ since we know that $0 < a^2 + b^2 < 2n$. □

Here is an additional explanation that why it is sufficient to prove under the case that $\gcd(x, y) = 1$ in the $Proof$ ($\Rightarrow$). There are three cases for x and y as follows:

$$\text{(i) } x = 0 \text{ or } y = 0 \quad \text{(ii) } \gcd(x, y) = 1 \quad \text{(iii) } \gcd(x, y) = d\,(> 1).$$

In the first case, $n = 0$ since x, y and z not all are 0. The third case becomes the same as the second case by dividing both sides of the equation $x^2+y^2 = nz^2$ by d. Thus, it is sufficient to prove under the case that $\gcd(x, y) = 1$ in the $Proof$ ($\Rightarrow$).

References

[1] https://medium.com/cantors-paradise/the-pigeonhole-principle-e4c637940619
[2] alamy.com/stock-photo/by-jean-leurechon.html
[3] en.wikipedia.org/wiki/Jean Leurechon
[4] ko.wikipedia.org/wiki/비둘기집 원리
[5] ko.wikipedia.org/wiki/페터 구스타프 르죈 디리클레
[6] https://mathworld.wolfram.com/DirichletsBoxPrinciple.html

Jaeik Choi, Department of Mathematics, Kwangwoon University, Seoul 01897, Republic of Korea
Email address: eikjae@naver.com