A lemma for B-R-C theorem

Some integral properties for the proof of B-R-C theorem
Seminars in Combinatorics

Jae-Ik Choi
Dept. of Math. in KWU

2020 Fall

What is the Pigeonhole property?

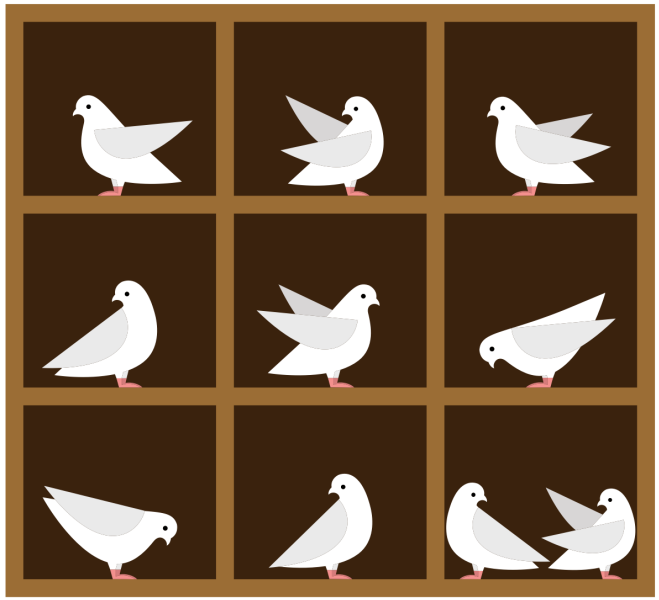

Figure: 10 pigeons and 9 pigeonholes

Theorem

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

Johann Peter Gustav Lejeune Dirichlet

Figure: Dirichlet (1805-1859)

- German mathematician
- number theory, mathematical analysis
- Dirichlet's Box Principle

Proof of the Pigeonhole property

Theorem

If n items are put into m containers, with $n > m$, then at least one container must contain more than one item.

Proof.

- Suppose that $\exists\, n+1$ items and $\exists\, n$ containers.
- Assume that each container contains no more than one item.
- Then there are at most n items in the containers.
- Contradiction!
- Thus, at least one container must contain more than one item.

A lemma for B-R-C theorem in number theory

Lemma

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 $a, b \in \mathbb{N}$.

- In this lemma, $0 \in \mathbb{N}$. ($n = 1$, $x = 3$, $y = 4$, $z = 5$.)
- x, y and z are not zero at the same time. ($n = 3$, $x = y = z = 0$.)
- Pigeonhole property is useful when we prove this lemma.
- This lemma is needed to prove the B-R-C Theorem.

Proof of the lemma

Lemma

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 $a, b \in \mathbb{N}$.

Proof. ($\Leftarrow$)

- Suppose that $n = a^2 + b^2$ for $a, b \in \mathbb{N}$.
- Then $nz^2 = (a^2 + b^2)z^2 = (az)^2 + (bz)^2$ where $z \in \mathbb{Z}$.
- Let $x = az$, $y = bz$. Then $nz^2 = x^2 + y^2$.
- We know that $n \in \mathbb{N}, x \in \mathbb{Z}$ and $y \in \mathbb{Z}$.
- Done!

Proof of the lemma

Lemma

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 $a, b \in \mathbb{N}$.

Proof. ($\Rightarrow$)

- Suppose that for some $n \in \mathbb{N}$ and $x, y, z \in \mathbb{Z}$, we have $x^2 + y^2 = nz^2$
- Suppose that $\gcd(x, y) = 1$. ($\Rightarrow \gcd(x, n) = 1$)
- Suppose that n is not a square.
- There uniquely exists $t \in \mathbb{N}$ such that $t^2 < n < (t+1)^2$.
- There are $(t+1)^2$ integer of the form $xu + yv$ with $0 \leq u, v \leq t$.
- 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 $x(u - u') + y(v - v') \equiv 0 \pmod{n}$.

Proof of the lemma

Lemma

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 $a, b \in \mathbb{N}$.

Proof. ($\Rightarrow$)

- Rewrite that $a = u - u', b = v - v'$.
- Then $|a|, |b| \leq t$. ($\Rightarrow 0 < a^2 + b^2 < 2n$)
- We get $xa + yb \equiv 0 \pmod{n}$
- This implies $x^2a^2 - y^2b^2 \equiv 0 \pmod{n}$.
- We know that $x^2b^2 + y^2b^2 \equiv 0 \pmod{n}$.
- Thus, $n \mid x^2(a^2 + b^2)$.
- We get $n \mid (a^2 + b^2)$. ($\because \gcd(x, n) = 1$)
- Therefore, $n = a^2 + b^2$. ($\because 0 < a^2 + b^2 < 2n$) Done!

Does the assumption is appropriate?

Lemma

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 $a, b \in \mathbb{N}$.

Problem

In the proof ($\Rightarrow$),

We suppose that $gcd(x, y) = 1$. ($\Rightarrow$ $gcd(x, n) = 1$)

We need to make sure that the above assumption is appropriate.

Does the assumption is appropriate?

Lemma

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 $a, b \in \mathbb{N}$.

Asssumption : We suppose that $\gcd(x, y) = 1$. ($\Rightarrow \gcd(x, n) = 1$)

Other case 1.

- If $\gcd(x, y) = d > 1$, let $x = dx_1$ and $y = dy_1$.
- We can rewrite that $d^2(x_1^2 + y_1^2) = nz^2$.
- This implies that $d^2 \mid nz^2$.
- Let $nz^2 = d^2k$ where $k \in \mathbb{N}$.
- Thus, we get $x_1^2 + y_1^2 = k(1)^2$ where $\gcd(x_1, y_1) = 1$.
- Done!

Does the assumption is appropriate?

Lemma

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 $a, b \in \mathbb{N}$.

Asssumption : We suppose that $\gcd(x, y) = 1$. ($\Rightarrow \gcd(x, n) = 1$)

Other case 2.

- Let $x = 0$ or $y = 0$.
- If $x = 0$ and $y \neq 0$, then $y^2 = nz^2$. ($\Rightarrow n = a^2$ for some $a \in \mathbb{N}$.)
- If $x = y = 0$, then $n = 0 = 0^2 + 0^2$.
- Done!

$\gcd(x, y) = 1 \Rightarrow \gcd(x, n) = 1$

Lemma

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 $a, b \in \mathbb{N}$.

Asssumption : We suppose that $\gcd(x, y) = 1$. ($\Rightarrow \gcd(x, n) = 1$)

- We will prove the contrapositive statement.
- Let $\gcd(x, n) = d > 1$.
- Then $d \mid y^2$.
- If d is a prime, let $d = p$. then $p \mid y$.
- If d is a composite, then $\exists$ a prime p such that $p \mid d$ ($\Rightarrow p \mid y$).
- This implies $\gcd(x, y) \geq p$ for a prime p.
- Done!

Lemma which is proved

Lemma

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 $a, b \in \mathbb{N}$.

- In this lemma, $0 \in \mathbb{N}$.
- x, y and z are not zero at the same time.
- This lemma is needed to prove the B-R-C Theorem.

More story about the Pigeonhole property

Theorem

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

- This property used to find the Ramsey number. (upper bound)
- This property used in the proof of Fermat's Little Theorem.
- This property has important applications in number theory.
- 모든 파일을 임의의 크기 S 이하로 압축하는 비손실 압축 알고리즘은 존재하지 않는다.

More story about the Pigeonhole property

Theorem

There is no algorithm that compresses all files to size S or less without loss.

Proof.

- Assume that there is an algorithm satisfying the above conditions.
- The number of files of size S or less are finite. (*Finite Pigeonholes*)
- The number of all files are infinite. (*Infinite Pigeons*)
- This implies that two different files compressed into the same file X.
- Thus, file X must be damaged when uncompressed.
- Therefore, there is *no algorithm* satisfying the above conditions.

□

Reference

- https://medium.com/cantors-paradise/the-pigeonhole-principle-e4c637940619
- ko.wikipedia.org/wiki/비둘기집 원리
- ko.wikipedia.org/wiki/페터 구스타프 르죈 디리클레
- https://mathworld.wolfram.com/DirichletsBoxPrinciple.html