

# Involutions2Squares

Maksym Bortin

March 8, 2026

## Abstract

This theory contains the involution-based proof of the ‘two squares’ theorem from [THE BOOK](#).

## Contents

<b>1</b>	<b>A few basic properties</b>	<b>1</b>
<b>2</b>	<b>The relevant properties of involutions</b>	<b>2</b>
2.1	Unions of preimage/image sets, fixed points . . . . .	2
<b>3</b>	<b>Primes and the two squares theorem</b>	<b>4</b>

```
theory Involutions2Squares
imports Main
begin
```

## 1 A few basic properties

```
lemma nat-sqr :
  shows  $\text{nat}(n^2) = (\text{nat}(\text{abs } n))^2$ 
  <proof>
```

```
lemma nat-mod-int :
  assumes  $n \bmod m = k$ 
  shows  $\text{int } n \bmod \text{int } m = \text{int } k$ 
  <proof>
```

```
lemma sqr-geq-nat :
  shows  $(n::\text{nat}) \leq n^2$ 
  <proof>
```

**lemma** *sqr-geq-abs* :  
  **shows**  $\text{abs}(n::\text{int}) \leq n^2$   
  ⟨*proof*⟩

**lemma** *sqr-fix-nat* :  
  **assumes**  $(n::\text{nat}) = n^2$   
  **shows**  $n = 0 \vee n = 1$   
  ⟨*proof*⟩

**lemma** *card1* :  
  **shows**  $(\text{card}\{a, b\} = \text{Suc } 0) = (a = b)$   
  ⟨*proof*⟩

**lemma** *card2* :  
  **shows**  $\text{card}\{a, b\} \geq \text{Suc } 0 \wedge \text{card}\{a, b\} \leq 2$   
  ⟨*proof*⟩

## 2 The relevant properties of involutions

**definition** *involution-on*  $A \varphi = (\varphi ' A \subseteq A \wedge (\forall x \in A. \varphi(\varphi x) = x))$

**lemma** *involution-bij* :  
  **assumes** *involution-on*  $A \varphi$   
  **shows** *bij-betw*  $\varphi A A$   
  ⟨*proof*⟩

**lemma** *involution-sub-bij* :  
  **assumes** *involution-on*  $A \varphi$   
    **and**  $S \subseteq A$   
    **and**  $\forall x \in A. (x \in S) = (\varphi x \notin S)$   
  **shows** *bij-betw*  $\varphi S (A - S)$   
  ⟨*proof*⟩

**lemma** *involution-sub-card* :  
  **assumes** *involution-on*  $A \varphi$   
    **and** *finite*  $A$   
    **and**  $S \subseteq A$   
    **and**  $\forall x \in A. (x \in S) = (\varphi x \notin S)$   
  **shows**  $2 * \text{card } S = \text{card } A$   
  ⟨*proof*⟩

## 2.1 Unions of preimage/image sets, fixed points

**definition** *preimg-img-on*  $A \varphi = (\bigcup x \in A. \{\{x, \varphi x\}\})$

**definition** *fixpoints-on*  $A \varphi = \{x \in A. \varphi x = x\}$

**lemma** *preimg-img-on-Union* :

**assumes**  $\varphi ' A \subseteq A$

**shows**  $A = \bigcup (\text{preimg-img-on } A \varphi)$

*<proof>*

**lemma** *preimg-img-on-finite* :

**assumes** *finite*  $A$

**shows** *finite*  $(\text{preimg-img-on } A \varphi)$

*<proof>*

**lemma** *fixpoints-on-finite* :

**assumes** *finite*  $A$

**shows** *finite*  $(\text{fixpoints-on } A \varphi)$

*<proof>*

**lemma** *preimg-img-on-card* :

**assumes**  $x \in \text{preimg-img-on } A \varphi$

**shows**  $1 \leq \text{card } x \wedge \text{card } x \leq 2$

*<proof>*

**corollary** *preimg-img-on-eq* :

**shows**  $\text{preimg-img-on } A \varphi = \{x \in \text{preimg-img-on } A \varphi. \text{card } x = 1\} \cup$   
 $\{x \in \text{preimg-img-on } A \varphi. \text{card } x = 2\}$

*<proof>*

**lemma** *fixpoints-on-card-eq* :

**shows**  $\text{card}(\text{fixpoints-on } A \varphi) = \text{card} \{x \in \text{preimg-img-on } A \varphi. \text{card } x = 1\}$

*<proof>*

**lemma** *preimg-img-on-disjoint* :

**assumes** *involution-on*  $A \varphi$

**shows** *pairwise disjnt*  $(\text{preimg-img-on } A \varphi)$

*<proof>*

**theorem** *involution-dom-card-sum* :

**assumes** *involution-on*  $A \varphi$

**and** *finite*  $A$

**shows**  $\text{card } A = \text{card}(\text{fixpoints-on } A \varphi) +$

$2 * \text{card } \{x \in \text{preimg-img-on } A \ \varphi. \ \text{card } x = 2\}$   
<proof>

**corollary** *involution-dom-fixpoints-parity* :  
  **assumes** *involution-on*  $A \ \varphi$   
  **and** *finite*  $A$   
  **shows**  $\text{odd}(\text{card } A) = \text{odd}(\text{card}(\text{fixpoints-on } A \ \varphi))$   
<proof>

### 3 Primes and the two squares theorem

**definition** *is-prime*  $(n :: \text{nat}) = (n > 1 \wedge (\forall d. d \ \text{dvd} \ n \longrightarrow d = 1 \vee d = n))$

**lemma** *prime-factors* :  
  **assumes** *is-prime*  $p$   
  **and**  $p = n * m$   
  **shows**  $(n = 1 \wedge m = p) \vee (n = p \wedge m = 1)$   
<proof>

**lemma** *prime-not-sqr* :  
  **assumes** *is-prime*  $p$   
  **shows**  $p \neq n^2$   
<proof>

**lemma** *int-prime-not-sqr* :  
  **assumes** *is-prime*  $p$   
  **shows**  $\text{int } p \neq n^2$   
<proof>

**lemma** *prime-gr4* :  
  **assumes** *is-prime*  $p$   
  **and**  $p \ \text{mod} \ 4 = 1$   
  **shows**  $p > 4$   
<proof>

**theorem** *two-squares* :  
  **assumes**  $a$ : *is-prime*  $p$   
  **and**  $b$ :  $p \ \text{mod} \ 4 = 1$   
  **shows**  $\exists n \ m. p = n^2 + m^2$   
<proof>

end