| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/EllipticCurve.html) | [**Tree**](http://docs.google.com/package-tree.html) | [**Deprecated**](http://docs.google.com/deprecated-list.html) | [**Index**](http://docs.google.com/index-files/index-1.html) | [**Help**](http://docs.google.com/help-doc.html) | | --- | --- | --- | --- | --- | --- | --- | --- | | | ***Java™ Platform***  ***Standard Ed. 6*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**PREV CLASS**](http://docs.google.com/java/security/spec/ECPublicKeySpec.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/EncodedKeySpec.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/EllipticCurve.html)    [**NO FRAMES**](http://docs.google.com/EllipticCurve.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#3dy6vkm) | [METHOD](#2s8eyo1) |

## **java.security.spec**

Class EllipticCurve

[java.lang.Object](http://docs.google.com/java/lang/Object.html)  
 **java.security.spec.EllipticCurve**

public class **EllipticCurve**extends [Object](http://docs.google.com/java/lang/Object.html)

This immutable class holds the necessary values needed to represent an elliptic curve.

**Since:** 1.5 **See Also:**[ECField](http://docs.google.com/java/security/spec/ECField.html), [ECFieldFp](http://docs.google.com/java/security/spec/ECFieldFp.html), [ECFieldF2m](http://docs.google.com/java/security/spec/ECFieldF2m.html)

| **Constructor Summary** | |
| --- | --- |
| [**EllipticCurve**](http://docs.google.com/java/security/spec/EllipticCurve.html#EllipticCurve(java.security.spec.ECField,%20java.math.BigInteger,%20java.math.BigInteger))([ECField](http://docs.google.com/java/security/spec/ECField.html) field, [BigInteger](http://docs.google.com/java/math/BigInteger.html) a, [BigInteger](http://docs.google.com/java/math/BigInteger.html) b)            Creates an elliptic curve with the specified elliptic field field and the coefficients a and b. |
| [**EllipticCurve**](http://docs.google.com/java/security/spec/EllipticCurve.html#EllipticCurve(java.security.spec.ECField,%20java.math.BigInteger,%20java.math.BigInteger,%20byte%5B%5D))([ECField](http://docs.google.com/java/security/spec/ECField.html) field, [BigInteger](http://docs.google.com/java/math/BigInteger.html) a, [BigInteger](http://docs.google.com/java/math/BigInteger.html) b, byte[] seed)            Creates an elliptic curve with the specified elliptic field field, the coefficients a and b, and the seed used for curve generation. |

| **Method Summary** | |
| --- | --- |
| boolean | [**equals**](http://docs.google.com/java/security/spec/EllipticCurve.html#equals(java.lang.Object))([Object](http://docs.google.com/java/lang/Object.html) obj)            Compares this elliptic curve for equality with the specified object. |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getA**](http://docs.google.com/java/security/spec/EllipticCurve.html#getA())()            Returns the first coefficient a of the elliptic curve. |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getB**](http://docs.google.com/java/security/spec/EllipticCurve.html#getB())()            Returns the second coefficient b of the elliptic curve. |
| [ECField](http://docs.google.com/java/security/spec/ECField.html) | [**getField**](http://docs.google.com/java/security/spec/EllipticCurve.html#getField())()            Returns the finite field field that this elliptic curve is over. |
| byte[] | [**getSeed**](http://docs.google.com/java/security/spec/EllipticCurve.html#getSeed())()            Returns the seeding bytes seed used during curve generation. |
| int | [**hashCode**](http://docs.google.com/java/security/spec/EllipticCurve.html#hashCode())()            Returns a hash code value for this elliptic curve. |

| **Methods inherited from class java.lang.**[**Object**](http://docs.google.com/java/lang/Object.html) |
| --- |
| [clone](http://docs.google.com/java/lang/Object.html#clone()), [finalize](http://docs.google.com/java/lang/Object.html#finalize()), [getClass](http://docs.google.com/java/lang/Object.html#getClass()), [notify](http://docs.google.com/java/lang/Object.html#notify()), [notifyAll](http://docs.google.com/java/lang/Object.html#notifyAll()), [toString](http://docs.google.com/java/lang/Object.html#toString()), [wait](http://docs.google.com/java/lang/Object.html#wait()), [wait](http://docs.google.com/java/lang/Object.html#wait(long)), [wait](http://docs.google.com/java/lang/Object.html#wait(long,%20int)) |

| **Constructor Detail** |
| --- |

### EllipticCurve

public **EllipticCurve**([ECField](http://docs.google.com/java/security/spec/ECField.html) field,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) a,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) b)

Creates an elliptic curve with the specified elliptic field field and the coefficients a and b.

**Parameters:**field - the finite field that this elliptic curve is over.a - the first coefficient of this elliptic curve.b - the second coefficient of this elliptic curve. **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if field, a, or b is null. [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if a or b is not null and not in field.

### EllipticCurve

public **EllipticCurve**([ECField](http://docs.google.com/java/security/spec/ECField.html) field,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) a,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) b,  
 byte[] seed)

Creates an elliptic curve with the specified elliptic field field, the coefficients a and b, and the seed used for curve generation.

**Parameters:**field - the finite field that this elliptic curve is over.a - the first coefficient of this elliptic curve.b - the second coefficient of this elliptic curve.seed - the bytes used during curve generation for later validation. Contents of this array are copied to protect against subsequent modification. **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if field, a, or b is null. [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if a or b is not null and not in field.

| **Method Detail** |
| --- |

### getField

public [ECField](http://docs.google.com/java/security/spec/ECField.html) **getField**()

Returns the finite field field that this elliptic curve is over.

**Returns:**the field field that this curve is over.

### getA

public [BigInteger](http://docs.google.com/java/math/BigInteger.html) **getA**()

Returns the first coefficient a of the elliptic curve.

**Returns:**the first coefficient a.

### getB

public [BigInteger](http://docs.google.com/java/math/BigInteger.html) **getB**()

Returns the second coefficient b of the elliptic curve.

**Returns:**the second coefficient b.

### getSeed

public byte[] **getSeed**()

Returns the seeding bytes seed used during curve generation. May be null if not specified.

**Returns:**the seeding bytes seed. A new array is returned each time this method is called.

### equals

public boolean **equals**([Object](http://docs.google.com/java/lang/Object.html) obj)

Compares this elliptic curve for equality with the specified object.

**Overrides:**[equals](http://docs.google.com/java/lang/Object.html#equals(java.lang.Object)) in class [Object](http://docs.google.com/java/lang/Object.html) **Parameters:**obj - the object to be compared. **Returns:**true if obj is an instance of EllipticCurve and the field, A, B, and seeding bytes match, false otherwise.**See Also:**[Object.hashCode()](http://docs.google.com/java/lang/Object.html#hashCode()), [Hashtable](http://docs.google.com/java/util/Hashtable.html)

### hashCode

public int **hashCode**()

Returns a hash code value for this elliptic curve.

**Overrides:**[hashCode](http://docs.google.com/java/lang/Object.html#hashCode()) in class [Object](http://docs.google.com/java/lang/Object.html) **Returns:**a hash code value.**See Also:**[Object.equals(java.lang.Object)](http://docs.google.com/java/lang/Object.html#equals(java.lang.Object)), [Hashtable](http://docs.google.com/java/util/Hashtable.html)

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/EllipticCurve.html) | [**Tree**](http://docs.google.com/package-tree.html) | [**Deprecated**](http://docs.google.com/deprecated-list.html) | [**Index**](http://docs.google.com/index-files/index-1.html) | [**Help**](http://docs.google.com/help-doc.html) | | --- | --- | --- | --- | --- | --- | --- | --- | | | ***Java™ Platform***  ***Standard Ed. 6*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**PREV CLASS**](http://docs.google.com/java/security/spec/ECPublicKeySpec.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/EncodedKeySpec.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/EllipticCurve.html)    [**NO FRAMES**](http://docs.google.com/EllipticCurve.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#3dy6vkm) | [METHOD](#2s8eyo1) |

[Submit a bug or feature](http://bugs.sun.com/services/bugreport/index.jsp)

For further API reference and developer documentation, see [Java SE Developer Documentation](http://docs.google.com/webnotes/devdocs-vs-specs.html). That documentation contains more detailed, developer-targeted descriptions, with conceptual overviews, definitions of terms, workarounds, and working code examples.

Copyright 2006 Sun Microsystems, Inc. All rights reserved. Use is subject to [license terms](http://docs.google.com/legal/license.html). Also see the [documentation redistribution policy](http://java.sun.com/docs/redist.html).