| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/ECFieldF2m.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/ECField.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/ECFieldFp.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/ECFieldF2m.html)    [**NO FRAMES**](http://docs.google.com/ECFieldF2m.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#3dy6vkm) | [METHOD](#17dp8vu) |

## **java.security.spec**

Class ECFieldF2m

[java.lang.Object](http://docs.google.com/java/lang/Object.html)  
 **java.security.spec.ECFieldF2m**

**All Implemented Interfaces:** [ECField](http://docs.google.com/java/security/spec/ECField.html)

public class **ECFieldF2m**extends [Object](http://docs.google.com/java/lang/Object.html)implements [ECField](http://docs.google.com/java/security/spec/ECField.html)

This immutable class defines an elliptic curve (EC) characteristic 2 finite field.

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

| **Constructor Summary** | |
| --- | --- |
| [**ECFieldF2m**](http://docs.google.com/java/security/spec/ECFieldF2m.html#ECFieldF2m(int))(int m)            Creates an elliptic curve characteristic 2 finite field which has 2^m elements with normal basis. |
| [**ECFieldF2m**](http://docs.google.com/java/security/spec/ECFieldF2m.html#ECFieldF2m(int,%20java.math.BigInteger))(int m, [BigInteger](http://docs.google.com/java/math/BigInteger.html) rp)            Creates an elliptic curve characteristic 2 finite field which has 2^m elements with polynomial basis. |
| [**ECFieldF2m**](http://docs.google.com/java/security/spec/ECFieldF2m.html#ECFieldF2m(int,%20int%5B%5D))(int m, int[] ks)            Creates an elliptic curve characteristic 2 finite field which has 2^m elements with polynomial basis. |

| **Method Summary** | |
| --- | --- |
| boolean | [**equals**](http://docs.google.com/java/security/spec/ECFieldF2m.html#equals(java.lang.Object))([Object](http://docs.google.com/java/lang/Object.html) obj)            Compares this finite field for equality with the specified object. |
| int | [**getFieldSize**](http://docs.google.com/java/security/spec/ECFieldF2m.html#getFieldSize())()            Returns the field size in bits which is m for this characteristic 2 finite field. |
| int | [**getM**](http://docs.google.com/java/security/spec/ECFieldF2m.html#getM())()            Returns the value m of this characteristic 2 finite field. |
| int[] | [**getMidTermsOfReductionPolynomial**](http://docs.google.com/java/security/spec/ECFieldF2m.html#getMidTermsOfReductionPolynomial())()            Returns an integer array which contains the order of the middle term(s) of the reduction polynomial for polynomial basis or null for normal basis. |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getReductionPolynomial**](http://docs.google.com/java/security/spec/ECFieldF2m.html#getReductionPolynomial())()            Returns a BigInteger whose i-th bit corresponds to the i-th coefficient of the reduction polynomial for polynomial basis or null for normal basis. |
| int | [**hashCode**](http://docs.google.com/java/security/spec/ECFieldF2m.html#hashCode())()            Returns a hash code value for this characteristic 2 finite field. |

| **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** |
| --- |

### ECFieldF2m

public **ECFieldF2m**(int m)

Creates an elliptic curve characteristic 2 finite field which has 2^m elements with normal basis.

**Parameters:**m - with 2^m being the number of elements. **Throws:** [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if m is not positive.

### ECFieldF2m

public **ECFieldF2m**(int m,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) rp)

Creates an elliptic curve characteristic 2 finite field which has 2^m elements with polynomial basis. The reduction polynomial for this field is based on rp whose i-th bit correspondes to the i-th coefficient of the reduction polynomial.

Note: A valid reduction polynomial is either a trinomial (X^m + X^k + 1 with m > k >= 1) or a pentanomial (X^m + X^k3 + X^k2 + X^k1 + 1 with m > k3 > k2 > k1 >= 1).

**Parameters:**m - with 2^m being the number of elements.rp - the BigInteger whose i-th bit corresponds to the i-th coefficient of the reduction polynomial. **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if rp is null. [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if m is not positive, or rp does not represent a valid reduction polynomial.

### ECFieldF2m

public **ECFieldF2m**(int m,  
 int[] ks)

Creates an elliptic curve characteristic 2 finite field which has 2^m elements with polynomial basis. The reduction polynomial for this field is based on ks whose content contains the order of the middle term(s) of the reduction polynomial. Note: A valid reduction polynomial is either a trinomial (X^m + X^k + 1 with m > k >= 1) or a pentanomial (X^m + X^k3 + X^k2 + X^k1 + 1 with m > k3 > k2 > k1 >= 1), so ks should have length 1 or 3.

**Parameters:**m - with 2^m being the number of elements.ks - the order of the middle term(s) of the reduction polynomial. Contents of this array are copied to protect against subsequent modification. **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if ks is null. [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - ifm is not positive, or the length of ks is neither 1 nor 3, or values in ks are not between m-1 and 1 (inclusive) and in descending order.

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

### getFieldSize

public int **getFieldSize**()

Returns the field size in bits which is m for this characteristic 2 finite field.

**Specified by:**[getFieldSize](http://docs.google.com/java/security/spec/ECField.html#getFieldSize()) in interface [ECField](http://docs.google.com/java/security/spec/ECField.html) **Returns:**the field size in bits.

### getM

public int **getM**()

Returns the value m of this characteristic 2 finite field.

**Returns:**m with 2^m being the number of elements.

### getReductionPolynomial

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

Returns a BigInteger whose i-th bit corresponds to the i-th coefficient of the reduction polynomial for polynomial basis or null for normal basis.

**Returns:**a BigInteger whose i-th bit corresponds to the i-th coefficient of the reduction polynomial for polynomial basis or null for normal basis.

### getMidTermsOfReductionPolynomial

public int[] **getMidTermsOfReductionPolynomial**()

Returns an integer array which contains the order of the middle term(s) of the reduction polynomial for polynomial basis or null for normal basis.

**Returns:**an integer array which contains the order of the middle term(s) of the reduction polynomial for polynomial basis or null for normal basis. 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 finite field 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 ECFieldF2m and both m and the reduction polynomial 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 characteristic 2 finite field.

**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/ECFieldF2m.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/ECField.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/ECFieldFp.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/ECFieldF2m.html)    [**NO FRAMES**](http://docs.google.com/ECFieldF2m.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#3dy6vkm) | [METHOD](#17dp8vu) |

[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).