**云南大学数学与与统计学院**

**上机实践报告**

|  |  |  |
| --- | --- | --- |
| **课程名称**：近代密码学实验 | **年级**：2013 | **上机实践成绩**： |
| **指导教师**：陆正福 | **姓名**：金洋 |  |
| **上机实践名称**：编程平台实验 | **学号**：20131910023 | **上机实践日期**：8.31 |
| **上机实践编号**：No.01 | **组号**： | **上机实践时间**： **16:25** |

**一、实验目的**

熟悉密码学编程平台和编程资源

1. **实验内容**
2. 阅读Java的BigInteger （java.math.BigInteger）和BigDecimal（java.math.BigDecimal）文档，分析两个类库的构成。自己构造例子熟悉BigInteger和BigDecimal中各个方法的使用
3. 在互联网查阅其它与密码学有关的编程资源，列出这些资源的网址，并予以简单介绍。

**三、实验环境**

个人计算机，Java 8平台

对于非信息与计算科学专业的学生，可以选择任意编程平台

**四、实验记录与实验结果分析**

（注意记录实验中遇到的问题。实验报告的评分依据之一是实验记录的细致程度、实验过程的真实性、实验结果的解释和分析。**如果涉及实验结果截屏，应选择白底黑字。**）

1. 阅读Java的BigInteger （java.math.BigInteger）和BigDecimal（java.math.BigDecimal）文档，分析两个类库的构成。自己构造例子熟悉BigInteger和BigDecimal中各个方法的使用

**(1) java.math.BigInteger**类提供操作类似所有Java的基本整数运算符和java.lang.Math中的所有相关的方法。

它还提供了模运算，GCD计算，素性测试，素数生成，位操作，和一些其他杂项业务操作。所有的操作行为，如果BigInteger的二进制补码委托表示法。

算术运算和按位逻辑运算的语义分别类似于那些Java的整数算术运算符和Java的按位整数运算符。移位操作的语义扩展那些Java的移位运算符的允许负移的距离。

比较操作执行有符号整数的比较。提供模块化的算术运算来计算残留，执行幂运算和计算乘法逆。位运算操作对他们的操作数的二进制补码表示的单个位。

在这个类将抛出NullPointerException，在所有方法和构造函数使用时，通过输入任何参数提供一个空的对象引用。

## 类声明

以下是java.math.BigInteger类的声明：

public class BigInteger

extends Number

implements Comparable<BigInteger>

## 字段域

以下是java.math.BigInteger类中的字段：

* static BigInteger ONE -- BigInteger的常量1。
* static BigInteger TEN -- BigInteger的常量10。
* static BigInteger ZERO -- BigInteger的常量0。

## 类构造函数

|  |  |
| --- | --- |
| **S.N.** | **构造函数 & 描述** |
| 1 | **BigInteger(byte[] val)** 这个构造函数用于转换一个字节数组包含BigInteger的二进制补码，以二进制表示成一个BigInteger。 |
| 2 | **BigInteger(int signum, byte[] magnitude)** 此构造函数用于将BigInteger的符号大小表示法转换成一个BigInteger值。 |
| 3 | **BigInteger(int bitLength, int certainty, Random rnd)** 此构造函数用于构造一个随机生成正BigInteger的可能是以指定的bitLength的素数。 |
| 4 | **BigInteger(int numBits, Random rnd)** 此构造函数用于构造一个随机生成的BigInteger，均匀分布在范围0到 (2numBits - 1), 包括. |
| 5 | **BigInteger(String val)** 此构造函数用于将BigInteger的十进制字符串表示形式转换成一个BigInteger值。 |
| 6 | **BigInteger(String val, int radix)** 这个构造函数用于转换为BigInteger的指定基数为一个BigInteger的字符串表示形式。 |

## 类方法

|  |  |
| --- | --- |
| **S.N.** | **方法 & 描述** |
| 1 | [BigInteger abs()](http://www.yiibai.com/java/math/biginteger_abs.html) 此方法返回一个BigInteger，其值是此BigInteger的绝对值。 |
| 2 | [BigInteger add(BigInteger val)](http://www.yiibai.com/java/math/biginteger_add.html) 此方法返回一个BigInteger，其值是(this + val). |
| 3 | [BigInteger and(BigInteger val)](http://www.yiibai.com/java/math/biginteger_and.html) 此方法返回一个BigInteger，其值是 (this & val). |
| 4 | [BigInteger andNot(BigInteger val)](http://www.yiibai.com/java/math/biginteger_andnot.html) 此方法返回一个BigInteger，其值是 (this & ~val). |
| 5 | [int bitCount()](http://www.yiibai.com/java/math/biginteger_bitcount.html) 此方法返回此BigInteger的二进制补码表示的位，从符号位不同的数字。 |
| 6 | [int bitLength()](http://www.yiibai.com/java/math/biginteger_bitlength.html) 此方法返回位在此BigInteger的最小的二进制补码表示的数，不包括符号位。 |
| 7 | [BigInteger clearBit(int n)](http://www.yiibai.com/java/math/biginteger_clearbit.html) 此方法返回一个BigInteger，其值相当于此BigInteger与指定位清零。 |
| 8 | [int compareTo(BigInteger val)](http://www.yiibai.com/java/math/biginteger_compareto.html) 此方法比较此BigInteger与指定的BigInteger。 |
| 9 | [BigInteger divide(BigInteger val)](http://www.yiibai.com/java/math/biginteger_divide.html) 此方法返回一个BigInteger，其值是 (this / val). |
| 10 | [BigInteger[ ] divideAndRemainder(BigInteger val)](http://www.yiibai.com/java/math/biginteger_divideandremainder.html) 此方法返回一个包含两个BigIntegers：(this / val) 和 (this % val)，其次是一个数组。 |
| 11 | [double doubleValue()](http://www.yiibai.com/java/math/biginteger_doublevalue.html) 此方法此BigInteger转换为双精度double。 |
| 12 | [boolean equals(Object x)](http://www.yiibai.com/java/math/biginteger_equals.html) 此方法比较此BigInteger与指定对象是否相等。 |
| 13 | [BigInteger flipBit(int n)](http://www.yiibai.com/java/math/biginteger_flipbit.html) 此方法返回一个BigInteger，其值相当于此BigInteger与指定位翻转。 |
| 14 | [float floatValue()](http://www.yiibai.com/java/math/biginteger_floatvalue.html) 此方法将BigInteger转换为float。 |
| 15 | [BigInteger gcd(BigInteger val)](http://www.yiibai.com/java/math/biginteger_gcd.html) 此方法返回一个BigInteger，其值是绝对值的最大公约数：abs(this) 和abs(val)。 |
| 16 | [int getLowestSetBit()](http://www.yiibai.com/java/math/biginteger_getlowestsetbit.html) 此方法返回最右边的（最低阶）的索引在此BigInteger1比特（零比特的数量，以最右侧的1位的右侧）。 |
| 17 | [int hashCode()](http://www.yiibai.com/java/math/biginteger_hashcode.html) 此方法返回此BigInteger的哈希代码。 |
| 18 | [int intValue()](http://www.yiibai.com/java/math/biginteger_intvalue.html) 此方法此BigInteger转换为int。 |
| 19 | [boolean isProbablePrime(int certainty)](http://www.yiibai.com/java/math/biginteger_isprobableprime.html) 此方法返回true，如果此BigInteger是素数，其绝对复合数则返回false。 |
| 20 | [long longValue()](http://www.yiibai.com/java/math/biginteger_longvalue.html) 些方法将BigInteger转换为long。 |
| 21 | [BigInteger max(BigInteger val)](http://www.yiibai.com/java/math/biginteger_max.html) 此方法返回此BigInteger和val的最大值。 |
| 22 | [BigInteger min(BigInteger val)](http://www.yiibai.com/java/math/biginteger_min.html) 此方法返回此BigInteger和val的最小值。 |
| 23 | [BigInteger mod(BigInteger m)](http://www.yiibai.com/java/math/biginteger_mod.html) 此方法返回一个BigInteger，其值是(this mod m). |
| 24 | [BigInteger modInverse(BigInteger m)](http://www.yiibai.com/java/math/biginteger_modinverse.html) 此方法返回一个BigInteger，其值是 (this-1 mod m). |
| 25 | [BigInteger modPow(BigInteger exponent, BigInteger m)](http://www.yiibai.com/java/math/biginteger_modpow.html) 此方法返回一个BigInteger，其值是 (thisexponent mod m). |
| 26 | [BigInteger multiply(BigInteger val)](http://www.yiibai.com/java/math/biginteger_multiply.html) 此方法返回一个BigInteger，其值是 (this \* val). |
| 27 | [BigInteger negate()](http://www.yiibai.com/java/math/biginteger_negate.html) 此方法返回一个BigInteger，其值是 (-this). |
| 28 | [BigInteger nextProbablePrime()](http://www.yiibai.com/java/math/biginteger_nextprobableprime.html) 此方法返回一个整数大于该BigInteger的可能是素数。 |
| 29 | [BigInteger not()](http://www.yiibai.com/java/math/biginteger_not.html) 此方法返回一个BigInteger，其值是 (~this). |
| 30 | [BigInteger or(BigInteger val)](http://www.yiibai.com/java/math/biginteger_or.html) 此方法返回一个BigInteger，其值是 (this | val). |
| 31 | [BigInteger pow(int exponent)](http://www.yiibai.com/java/math/biginteger_pow.html) 此方法返回一个BigInteger，其值是(thisexponent). |
| 32 | [static BigInteger probablePrime(int bitLength, Random rnd)](http://www.yiibai.com/java/math/biginteger_probableprime.html) 此方法返回一个正BigInteger的可能是素数，以指定的bitLength。 |
| 33 | [BigInteger remainder(BigInteger val)](http://www.yiibai.com/java/math/biginteger_remainder.html) 此方法返回一个BigInteger，其值是 (this % val). |
| 34 | [BigInteger setBit(int n)](http://www.yiibai.com/java/math/biginteger_setbit.html) 此方法返回一个BigInteger，其值相当于此BigInteger与指定的位设置。 |
| 35 | [BigInteger shiftLeft(int n)](http://www.yiibai.com/java/math/biginteger_shiftleft.html) 此方法返回一个BigInteger，其值是 (this << n). |
| 36 | [BigInteger shiftRight(int n)](http://www.yiibai.com/java/math/biginteger_shiftright.html) 此方法返回一个BigInteger，其值是 (this >> n). |
| 37 | [int signum()](http://www.yiibai.com/java/math/biginteger_signum.html) This method returns the signum function of this BigInteger. |
| 38 | [BigInteger subtract(BigInteger val)](http://www.yiibai.com/java/math/biginteger_subtract.html) 此方法返回一个BigInteger，其值是 (this - val). |
| 39 | [boolean testBit(int n)](http://www.yiibai.com/java/math/biginteger_testbit.html) 此方法返回当且仅当所指定的位被设置为真。 |
| 40 | [byte[ ] toByteArray()](http://www.yiibai.com/java/math/biginteger_tobytearray.html) 此方法返回一个包含此BigInteger的二进制补码表示的字节数组。 |
| 41 | [String toString()](http://www.yiibai.com/java/math/biginteger_tostring.html) 此方法返回此BigInteger的十进制字符串表示形式。 |
| 42 | [String toString(int radix)](http://www.yiibai.com/java/math/biginteger_tostring_radix.html) 此方法返回在给定的基数以BigInteger的字符串表示形式。 |
| 43 | [static BigInteger valueOf(long val)](http://www.yiibai.com/java/math/biginteger_valueof.html) 此方法返回一个BigInteger，其值等于指定long。 |
| 44 | [BigInteger xor(BigInteger val)](http://www.yiibai.com/java/math/biginteger_xor.html) 此方法返回一个BigInteger，其值是 (this ^ val). |

**(2) java.math.BigDecimal**类提供用于算术，刻度操作，舍入，比较，哈希算法和格式转换操作。

toString()方法提供BigDecimal的规范表示。它使用户可以完全控制舍入行为。

提供用于操作BigDecimal规模两种类型的操作：

* 缩放/舍入操作
* 小数点移动操作。

此类及其迭代器实现Comparable接口的所有可选方法。

## 类声明

以下是声明java.math.BigDecimal类：

public class BigDecimal

extends Number

implements Comparable<BigDecimal>

## 字段域

以下是java.math.BigDecimal类中的字段：

* static BigDecimal ONE -- 值为1，使用刻度为0。
* static int ROUND\_CEILING -- 舍入模式舍向正无穷。
* static int ROUND\_DOWN -- 舍入模式为向零舍入。
* static int ROUND\_FLOOR -- 舍入模式接近负无穷大。
* static int ROUND\_HALF\_DOWN -- 舍入模式舍入到“最近相邻”如果与两个相邻数字的距离相等，在这种情况下，向下取整。
* static int ROUND\_HALF\_EVEN --  舍入模式舍对“近邻”如果与两个相邻数字的距离相等，在这种情况下，舍入向着更加相邻。
* static int ROUND\_HALF\_UP -- 舍入模式舍入到“最近相邻”如果与两个相邻数字的距离相等，在这种情况下范围。
* static int ROUND\_UNNECESSARY -- 舍入模式断言请求的操作具有精确的结果，因此不需要舍入。
* static int ROUND\_UP -- 舍入模式舍入去零。
* static BigDecimal TEN -- 值为0，使用刻度为0。
* static BigDecimal ZERO -- 值为0，使用刻度为0。

## 类构造函数

|  |  |
| --- | --- |
| **S.N.** | **构造函数 & 描述** |
| 1 | **BigDecimal(BigInteger val)** 这个构造函数是用来将BigInteger转换为BigDecimal。 |
| 2 | **BigDecimal(BigInteger unscaledVal, int scale)** 这个构造函数用于转换为BigInteger非标度值和一个int尺度成一个BigDecimal。 |
| 3 | **BigDecimal(BigInteger unscaledVal, int scale, MathContext mc)** 这个构造函数用于转换为BigInteger非标度值和一个int尺度转换为BigDecimal，有根据上下文设置进行舍入。 |
| 4 | **BigDecimal(BigInteger val, MathContext mc)** 此构造函数用于根据上下文设置将BigInteger转换为BigDecimal舍入。 |
| 5 | **BigDecimal(char[ ] in)** 此构造函数用于将BigDecimal字符数组表示转化为BigDecimal，接受相同的字符序列与BigDecimal（String）构造函数。 |
| 6 | **BigDecimal(char[ ] in, int offset, int len)** 此构造函数用于将BigDecimal的字符数组表示转化为BigDecimal，接受字符与BigDecimal（String）构造方法相同的字符序列，同时允许指定子数组。 |
| 7 | **BigDecimal(char[ ] in, int offset, int len, MathContext mc)** 此构造函数用于将BigDecimal的字符数组表示转化为BigDecimal，接受字符与BigDecimal（String）构造方法相同的字符序列，同时允许指定子数组，并与根据上下文设置进行舍入。 |
| 8 | **BigDecimal(char[ ] in, MathContext mc)** 此构造函数用于将BigDecimal的字符数组表示转化为BigDecimal，接受相同的字符序列与BigDecimal（String）构造和根据上下文设置进行舍入。 |
| 9 | **BigDecimal(double val)** 这个构造函数是用来转换double为一个BigDecimal，它是双的二进制浮点值的精确十进制表示。 |
| 10 | **BigDecimal(double val, MathContext mc)** 这个构造函数是用来转换double为一个BigDecimal，有根据上下文设置进行舍入。 |
| 11 | **BigDecimal(int val)** 这个构造函数是用来转换一个int转换为BigDecimal。 |
| 12 | **BigDecimal(int val, MathContext mc)** 这个构造函数是用来转换一个int转换为BigDecimal，有根据上下文设置进行舍入。 |
| 13 | **BigDecimal(long val)** 这个构造函数用于转换long为一个BigDecimal。 |
| 14 | **BigDecimal(long val, MathContext mc)** 这个构造函数是将BigInteger转换为BigDecimal。 |
| 15 | **BigDecimal(String val)** 此构造函数用于一个BigDecimal的字符串表示形式转换为BigDecimal。 |
| 16 | **BigDecimal(String val, MathContext mc)** 此构造函数用于将BigDecimal的字符串表示形式转换为BigDecimal，接受相同的字符串作为与BigDecimal（String）构造，并根据上下文设置进行舍入。 |

## 类方法

|  |  |
| --- | --- |
| **S.N.** | **方法 & 描述** |
| 1 | [BigDecimal abs()](http://www.yiibai.com/java/math/bigdecimal_abs.html) 此方法返回一个BigDecimal，其值是此BigDecimal的绝对值，其标度是this.scale()。 |
| 2 | [BigDecimal abs(MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_abs_mc.html) 此方法返回一个BigDecimal，其值是此BigDecimal的绝对值，与根据上下文设置进行舍入。 |
| 3 | [BigDecimal add(BigDecimal augend)](http://www.yiibai.com/java/math/bigdecimal_add_augend.html) 此方法返回一个BigDecimal，其值为(this + augend)，其标度为max(this.scale(), augend.scale())。 |
| 4 | [BigDecimal add(BigDecimal augend, MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_add_augend_mc.html) 此方法返回一个BigDecimal，其值为 (this + augend)，与根据上下文设置进行舍入。 |
| 5 | [byte byteValueExact()](http://www.yiibai.com/java/math/bigdecimal_bytevalueexact.html) 这种方法的BigDecimal转换为一个字节，检查丢失的信息。 |
| 6 | [int compareTo(BigDecimal val)](http://www.yiibai.com/java/math/bigdecimal_compareto.html) 这种方法比较BigDecimal与指定的BigDecimal。 |
| 7 | [BigDecimal divide(BigDecimal divisor)](http://www.yiibai.com/java/math/bigdecimal_divide.html) 此方法返回一个BigDecimal，其值为（this/除数），且其首选标度为（this.scale() - divisor.scale()）;如果准确的商不能表示（因为它有无穷的十进制扩展），则抛出ArithmeticException。 |
| 8 | [BigDecimal divide(BigDecimal divisor, int roundingMode)](http://www.yiibai.com/java/math/bigdecimal_divide_roundingmode.html) 此方法返回一个BigDecimal，其值为（this/除数），其标度是this.scale()。 |
| 9 | [BigDecimal divide(BigDecimal divisor, int scale, int roundingMode)](http://www.yiibai.com/java/math/bigdecimal_divide_introundingmode_scale.html) 此方法返回一个BigDecimal，其值为（this/除数），其标度如指定。 |
| 10 | [BigDecimal divide(BigDecimal divisor, int scale, RoundingMode roundingMode)](http://www.yiibai.com/java/math/bigdecimal_divide_rdroundingmode_scale.html) 此方法返回一个BigDecimal，其值为（this/除数），其标度为指定。 |
| 11 | [BigDecimal divide(BigDecimal divisor, MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_divide_mc.html) 此方法返回一个BigDecimal，其值为（this/除数），与根据上下文设置进行舍入。 |
| 12 | [BigDecimal divide(BigDecimal divisor, RoundingMode roundingMode)](http://www.yiibai.com/java/math/bigdecimal_divide_rdroundingmode.html) 此方法返回一个BigDecimal，其值为（this/除数），其标度是this.scale()。 |
| 13 | [BigDecimal[ ] divideAndRemainder(BigDecimal divisor)](http://www.yiibai.com/java/math/bigdecimal_divideandremainder.html) 这个方法返回一个包含divideToIntegralValue结果，其次是剩下的两个操作数的结果的结果由两个元素组成的BigDecimal数组。 |
| 14 | [BigDecimal[ ] divideAndRemainder(BigDecimal divisor, MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_divideandremainder_mc.html) 这个方法返回一个包含divideToIntegralValue的结果，随后其余与上根据上下文设置进行舍入计算两个操作数的结果的结果由两个元素组成的BigDecimal数组。 |
| 15 | [BigDecimal divideToIntegralValue(BigDecimal divisor)](http://www.yiibai.com/java/math/bigdecimal_dividetointegralvalue.html) 此方法返回一个BigDecimal，其值为商（这/除数）的整数部分四舍五入。 |
| 16 | [BigDecimal divideToIntegralValue(BigDecimal divisor, MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_divideintegralvalue_mc.html) 此方法返回一个BigDecimal，其值是（这/除数）的整数部分。 |
| 17 | [double doubleValue()](http://www.yiibai.com/java/math/bigdecimal_doublevalue.html) 此方法将BigDecimal转换为double。 |
| 18 | [boolean equals(Object x)](http://www.yiibai.com/java/math/bigdecimal_equals.html) 这种方法比较BigDecimal与指定对象是否相等。 |
| 19 | [float floatValue()](http://www.yiibai.com/java/math/bigdecimal_floatvalue.html) 这种方法将BigDecimal转换为float。 |
| 20 | [int hashCode()](http://www.yiibai.com/java/math/bigdecimal_hashcode.html) 此方法返回BigDecimal的哈希代码。 |
| 21 | [int intValue()](http://www.yiibai.com/java/math/bigdecimal_intvalue.html) 这种方法将BigDecimal转换为int。 |
| 22 | [int intValueExact()](http://www.yiibai.com/java/math/bigdecimal_intvalueexact.html) 这种方法将BigDecimal转换为int，检查丢失的信息。 |
| 23 | [long longValue()](http://www.yiibai.com/java/math/bigdecimal_longvalue.html) 这种方法将BigDecimal转换为long。 |
| 24 | [long longValueExact()](http://www.yiibai.com/java/math/bigdecimal_longvalueexact.html) 这种方法将BigDecimal转换为long，检查丢失的信息。 |
| 25 | [BigDecimal max(BigDecimal val)](http://www.yiibai.com/java/math/bigdecimal_max.html) 此方法返回此BigDecimal和val的最大值。 |
| 26 | [BigDecimal min(BigDecimal val)](http://www.yiibai.com/java/math/bigdecimal_min.html) 此方法返回此BigDecimal和val的最小值。 |
| 27 | [BigDecimal movePointLeft(int n)](http://www.yiibai.com/java/math/bigdecimal_movepointleft.html) 此方法返回一个BigDecimal，它等效于将该值的小数点移动n位到左边。 |
| 28 | [BigDecimal movePointRight(int n)](http://www.yiibai.com/java/math/bigdecimal_movepointright.html) 此方法返回一个BigDecimal，它等效于将该值的小数点移动n位到右边。 |
| 29 | [BigDecimal multiply(BigDecimal multiplicand)](http://www.yiibai.com/java/math/bigdecimal_multiply.html) 此方法返回一个BigDecimal，其值为（this×被乘数），其标度为（this.scale()+ multiplicand.scale()）。 |
| 30 | [BigDecimal multiply(BigDecimal multiplicand, MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_multiply_mc.html) 此方法返回一个BigDecimal，其值为（this×乘数），以根据上下文设置进行舍入。 |
| 31 | [BigDecimal negate()](http://www.yiibai.com/java/math/bigdecimal_negate.html) 此方法返回一个BigDecimal，其值是（+this），其标度是this.scale()。 |
| 32 | [BigDecimal negate(MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_negate_mc.html) 此方法返回一个BigDecimal，其值是（-this），根据上下文设置进行舍入。 |
| 33 | [BigDecimal plus()](http://www.yiibai.com/java/math/bigdecimal_plus.html) 此方法返回一个BigDecimal，其值是（+this），其标度是this.scale()。 |
| 34 | [BigDecimal plus(MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_plus_mc.html) 此方法返回一个BigDecimal，其值是（+this），根据上下文设置进行舍入。 |
| 35 | [BigDecimal pow(int n)](http://www.yiibai.com/java/math/bigdecimal_pow.html) 此方法返回一个BigDecimal，其值是(thisn), 幂被精确计算，使其具有无限精度。 |
| 36 | [BigDecimal pow(int n, MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_pow_mc.html) 此方法返回一个BigDecimal，其值是 (thisn). |
| 37 | [int precision()](http://www.yiibai.com/java/math/bigdecimal_precision.html) 此方法返回此BigDecimal的精度。 |
| 38 | [BigDecimal remainder(BigDecimal divisor)](http://www.yiibai.com/java/math/bigdecimal_remainder.html) 此方法将BigDecimal转换为一个byte，检查丢失的信息。 |
| 39 | [BigDecimal remainder(BigDecimal divisor, MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_remainder_mc.html) 此方法返回一个BigDecimal，其值为（this％除数），根据上下文设置进行舍入。 |
| 40 | [BigDecimal round(MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_round.html) 此方法返回根据MathContext设置舍入一个BigDecimal。 |
| 41 | [int scale()](http://www.yiibai.com/java/math/bigdecimal_scale.html) 此方法返回此BigDecimal的标度。 |
| 42 | [BigDecimal scaleByPowerOfTen(int n)](http://www.yiibai.com/java/math/bigdecimal_scalebypoweroften.html) 此方法返回一个BigDecimal，其数值等于 (this \* 10n). |
| 43 | [BigDecimal setScale(int newScale)](http://www.yiibai.com/java/math/bigdecimal_setscale.html) 此方法返回一个BigDecimal，其标度为指定值，其值在数值上等于该BigDecimal。 |
| 44 | [BigDecimal setScale(int newScale, int roundingMode)](http://www.yiibai.com/java/math/bigdecimal_setscale_roundingmode.html) 此方法返回一个BigDecimal，其标度为指定值，其非标度值乘以或除以此BigDecimal的非标度值除以十的次幂，以保持其整体值决定。 |
| 45 | [BigDecimal setScale(int newScale, RoundingMode roundingMode)](http://www.yiibai.com/java/math/bigdecimal_setscale_rm_roundingmode.html) 此方法返回一个BigDecimal，其标度为指定值，其非标度值乘以或除以此BigDecimal的非标度值除以十的次幂，以保持其整体价决定。 |
| 46 | [short shortValueExact()](http://www.yiibai.com/java/math/bigdecimal_shortvalueexact.html) 这种方法将BigDecimal转换为short，检查丢失的信息。 |
| 47 | [int signum()](http://www.yiibai.com/java/math/bigdecimal_signum.html) 此方法返回此BigDecimal的正负号函数。 |
| 48 | [BigDecimal stripTrailingZeros()](http://www.yiibai.com/java/math/bigdecimal_striptrailingzeros.html) 此方法返回一个BigDecimal，它在数值上等于这一个，但与从表示形式移除所有尾部零。 |
| 49 | [BigDecimal subtract(BigDecimal subtrahend)](http://www.yiibai.com/java/math/bigdecimal_subtract.html) 此方法返回一个BigDecimal，其值为（this - 减数），其标度为max（this.scale()，subtrahend.scale()）。 |
| 50 | [BigDecimal subtract(BigDecimal subtrahend, MathContext mc)](http://www.yiibai.com/java/math/bigdecimal_subtract_mc.html) 此方法返回一个BigDecimal，其值为（this - 减数），与根据上下文设置进行舍入。 |
| 51 | [BigInteger toBigInteger()](http://www.yiibai.com/java/math/bigdecimal_tobiginteger.html) 这种方法将BigDecimal转换为BigInteger。 |
| 52 | [BigInteger toBigIntegerExact()](http://www.yiibai.com/java/math/bigdecimal_tobigintegerexact.html) 这种方法将BigDecimal转换为BigInteger，检查丢失的信息。 |
| 53 | [String toEngineeringString()](http://www.yiibai.com/java/math/bigdecimal_toengineeringstring.html) 此方法返回此BigDecimal的字符串表示形式，使用工程计数法，如果需要指数。 |
| 54 | [String toPlainString()](http://www.yiibai.com/java/math/bigdecimal_toplainstring.html) 此方法返回此BigDecimal的字符串表示形式不带指数字段。 |
| 55 | [String toString()](http://www.yiibai.com/java/math/bigdecimal_tostring.html) 此方法返回此BigDecimal的字符串表示形式，用科学记数法，如果需要指数。 |
| 56 | [BigDecimal ulp()](http://www.yiibai.com/java/math/bigdecimal_ulp.html) 此方法返回一个ULP的此BigDecimal的大小，在最后一位的单位。 |
| 57 | [BigInteger unscaledValue()](http://www.yiibai.com/java/math/bigdecimal_unscaledvalue.html) 此方法返回一个BigInteger，其值是此BigDecimal的非标度值。 |
| 58 | [static BigDecimal valueOf(double val)](http://www.yiibai.com/java/math/bigdecimal_valueof_double.html) 这种方法转换double为一个BigDecimal，使用Double.toString（double）方法提供的double的规范化字符串表示形式。 |
| 59 | [static BigDecimal valueOf(long val)](http://www.yiibai.com/java/math/bigdecimal_valueof_long.html) 这种方法将一个long值转换为BigDecimal带有刻度的零值。 |
| 60 | [static BigDecimal valueOf(long unscaledVal, int scale)](http://www.yiibai.com/java/math/bigdecimal_valueof_scale.html) 这种方法转换long的非标度值和一个int尺度成一个BigDecimal。 |

(3) BigInteger基本方法熟悉

**package** MC01;

**import** java.math.BigInteger;

**import** java.util.Scanner;

**public** **class** TestBigInteger {

**public** **static** **void** main(String[] args) {

// **TODO** Auto-generated method stub

Scanner input=**new** Scanner(System.***in***);

BigInteger num1,num2;

System.***out***.print("num1=");num1=input.nextBigInteger();

System.***out***.print("num2=");num2=input.nextBigInteger();

System.***out***.println(num1+"+"+num2+"="+num1.add(num2));

System.***out***.println(num1+"-"+num2+"="+num1.subtract(num2));

System.***out***.println(num1+"\*"+num2+"="+num1.multiply(num2));

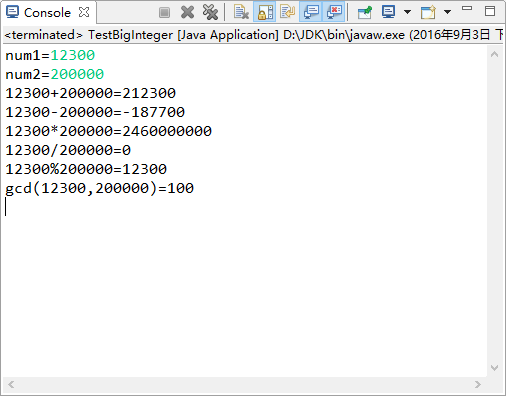
System.***out***.println(num1+"/"+num2+"="+num1.divide(num2));

System.***out***.println(num1+"%"+num2+"="+num1.mod(num2));

System.***out***.println("gcd("+num1+","+num2+")="+num1.gcd(num2));

}

}



1. BigDecimal基本方法熟悉

**package** MC01;

**import** java.math.BigDecimal;

**import** java.util.Scanner;

**public** **class** TestBigDecimal {

**public** **static** **void** main(String[] args) {

// **TODO** Auto-generated method stub

Scanner input=**new** Scanner(System.***in***);

BigDecimal num1,num2;

System.***out***.print("num1=");num1=input.nextBigDecimal();

System.***out***.print("num2=");num2=input.nextBigDecimal();

System.***out***.println(num1+"+"+num2+"="+num1.add(num2));

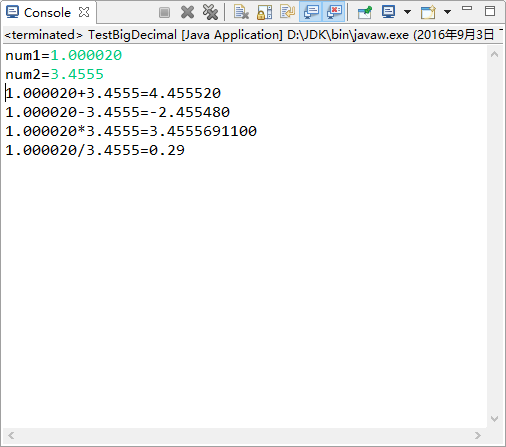
System.***out***.println(num1+"-"+num2+"="+num1.subtract(num2));

System.***out***.println(num1+"\*"+num2+"="+num1.multiply(num2));

System.***out***.println(num1+"/"+num2+"="+num1.divide(num2,2,BigDecimal.***ROUND\_HALF\_EVEN***));//保留2位小数，四舍五入

}

}



2.在互联网查阅其它与密码学有关的编程资源，列出这些资源的网址，并予以简单介绍。

<http://people.csail.mit.edu/rivest/publications.html> - 收集著名密码专家Ronald L. Rivest重要文献的网页。

<http://random.mat.sbg.ac.at/> - 萨尔茨堡大学数学系关于随机数生成理论和实践的主页。

<http://blog.csdn.net/aaaaatiger/article/details/2137302> - 收集了对密码学概述的网站和许多密码算法的文献。

<http://www.pediy.com/default.php> - 看雪论坛是个[软件安全](http://baike.baidu.com/view/2365355.htm" \t "http://baike.baidu.com/_blank)技术交流场所，为安全技术爱好者提供一个技术交流平台和资源。从单一版块『[软件调试](http://baike.baidu.com/view/272933.htm" \t "http://baike.baidu.com/_blank)论坛』，发展到以软件安全技术为主题多个版块的综合论坛。

<http://www.csdn.net/tag/%E5%AF%86%E7%A0%81%E5%AD%A6> - CSDN上的密码学专栏，但是内容不多

<http://book.51cto.com/art/200812/101258.htm> 《密码学与网络安全》电子书

<http://bbs.sciencenet.cn/forum.php?mod=forumdisplay&fid=108> sciencenet.cn 下的密码学专栏

<http://wenku.baidu.com/link?url=dFBSuZjBAMdktSoKVKzVwcHCMj2FXGITuliN-j0p4bRbzRAdl9Z0gtX1EkIAApp7kGxqKfT8dPTkqqomwnaQguU_7T05FHD7k2MVEYO6WN7> -密码学方面的国内外著名网站汇总

<http://crypto.stackexchange.com/questions>

<http://cstheory.stackexchange.com/> 两个国外的密码学网站，有大量数学问题，遗憾的是回答者比较少

<http://www.oracle.com/technetwork/java/javase/jaas/index.html> - Java SE Security

**五、实验体会**

**（请认真填写自己的真实体会）**

1.在BigInteger中有判断素数的方法：boolean isProbablePrime(int certainty)。如果此 BigInteger可能为素数，则返回true，如果它一定为合数，则返回false。如果certainty<= 0，则返回true。参数certainty是调用方允许的不确定性的度量。如果该调用返回true，则此 BigInteger 是素数的概率超出。此方法的执行时间与此参数的值是成比例的。

2. BigInteger与BigDecimal都是不可变的（immutable）的，在进行每一步运算时，都会产生一个新的对象，由于创建对象会引起开销，因此它们不适合于大量的数学运算，应尽量使用long、float、double等基本类型做科学计算或者工程计算。设计BigInteger与BigDecimal的目的是用来精确地表示大整数和小数，常用于商业计算中。

3. BigDecimal够造方法的参数类型有4种，其中的两个用BigInteger构造，另一个是用double构造，还有一个使用String构造。应该避免使用double构造BigDecimal，因为：有些数字用double根本无法精确表示，传给BigDecimal构造方法时就已经不精确了。比如，new BigDecimal(0.1)得到的值是0.1000000000000000055511151231257827021181583404541015625。使用new BigDecimal("0.1")得到的值是0.1。因此，如果需要精确计算，用String构造BigDecimal，避免用double构造，尽管它看起来更简单。

4. equals()方法认为0.1和0.1是相等的，返回true，而认为0.10和0.1是不等的，结果返回false。方法compareTo()则认为0.1与0.1相等，0.10与0.1也相等。所以在从数值上比较两个BigDecimal值时，应该使用compareTo()而不是 equals()。

5.另外还有一些情形，任意精度的小数运算仍不能表示精确结果。例如，1除以9会产生无限循环的小数 .111111...。出于这个原因，在进行除法运算时，BigDecimal可以显式地控制舍入。

6. java的float只能用来进行科学计算或工程计算，在大多数的商业计算中，一般采用java.math.BigDecimal类来进行精确计算。在使用BigDecimal类来进行计算的时候，主要分为以下步骤：  
①用float或者double变量构建BigDecimal对象。  
②通过调用BigDecimal的加，减，乘，除等相应的方法进行算术运算。  
③把BigDecimal对象转换成float，double，int等类型。

**六、参考文献**

1. <http://docs.oracle.com/javase/8/docs/api/>

**2.（如有其它参考文献，请列出）**