```java
import components.naturalnumber.NaturalNumber;
import components.naturalnumber.NaturalNumber2;
import components.random.Random;
import components.random.Random1L;
import components.simplereader.SimpleReader;
import components.simplereader.SimpleReader1L;
import components.simplewriter.SimpleWriter;
import components.simplewriter.SimpleWriter1L;

/**
 * Utilities that could be used with RSA cryptosystems.
 *
 * @author Ansh Pachauri
 *
 */
public final class CryptoUtilities {

    /**
     * Private constructor so this utility class cannot be instantiated.
     */
    private CryptoUtilities() {
    }

    /**
     * Useful constant, not a magic number: 3.
     */
    private static final int THREE = 3;

    /**
     * Pseudo-random number generator.
     */
    private static final Random GENERATOR = new Random1L();

    /**
     * Returns a random number uniformly distributed in the interval [0, n].
     *
     * @param n
     *            top end of interval
     * @return random number in interval
     * @requires n > 0
     * @ensures <pre>
     * randomNumber = [a random number uniformly distributed in [0, n]]
     * </pre>
     */
    public static NaturalNumber randomNumber(NaturalNumber n) {
        assert !n.isZero() : "Violation of: n > 0";
        final int base = 10;
        NaturalNumber result;
        int d = n.divideBy10();
        if (n.isZero()) {
            /*
             * Incoming n has only one digit and it is d, so generate a random
             * number uniformly distributed in [0, d]
             */
            int x = (int) ((d + 1) * GENERATOR.nextDouble());
            result = new NaturalNumber2(x);
            n.multiplyBy10(d);
        } else {
            /*
             * Incoming n has more than one digit, so generate a random number
             * (NaturalNumber) uniformly distributed in [0, n], and another
             * (int) uniformly distributed in [0, 9] (i.e., a random digit)
             */
            result = randomNumber(n);
            int lastDigit = (int) (base * GENERATOR.nextDouble());
            result.multiplyBy10(lastDigit);
            n.multiplyBy10(d);
            if (result.compareTo(n) > 0) {
                /*
                 * In this case, we need to try again because
```

```
generated number
                 * is greater than n; the recursive call's argument is not
                 * "smaller" than the incoming value of n, but this recursive
                 * call has no more than a 90% chance of being made (and for
                 * large n, far less than that), so the probability of
                 * termination is 1
                 */
                result = randomNumber(n);
            }
        }
        return result;
    }

    /**
     * Finds the greatest common divisor of n and m.
     *
     * @param n
     *            one number
     * @param m
     *            the other number
     * @updates n
     * @clears m
     * @ensures n = [greatest common divisor of #n and #m]
     */
    public static void reduceToGCD(NaturalNumber n, NaturalNumber m) {

        /*
         * Use Euclid's algorithm; in pseudocode: if m = 0 then GCD(n, m) = n
         * else GCD(n, m) = GCD(m, n mod m)
         */

        // TODO - fill in body
        NaturalNumber zero = new NaturalNumber2(0);
        if (!m.isZero()) {
            // Create new natural number k to hold value of n mod m
            NaturalNumber k = new NaturalNumber2(n.divide(m));
            reduceToGCD(m, k);
            // transferFrom m in order to update n and clear m
            n.transferFrom(m);
        }
    }

    /**
     * Reports whether n is even.
     *
     * @param n
     *            the number to be checked
     * @return true iff n is even
     * @ensures isEven = (n mod 2 = 0)
     */
    public static boolean isEven(NaturalNumber n) {

        // TODO - fill in body
        NaturalNumber temp = new NaturalNumber2(n);
        NaturalNumber two = new NaturalNumber2(2);
        boolean choice = false;
        //checking if n mod 2 is equal to 0
        if (temp.divide(two).isZero()) {
            choice = true;
        }

        return choice;
    }

    /**
     * Updates n to its p-th power modulo m.
     *
     * @param n
     *            number to be raised to a power
     * @param p
     *            the power
```

```java
     * @param m
     *            the modulus
     * @updates n
     * @requires m > 1
     * @ensures n = #n ^ (p) mod m
     */
    public static void powerMod(NaturalNumber n, NaturalNumber p,
            NaturalNumber m) {
        assert m.compareTo(new NaturalNumber2(1)) > 0 : "Violation of: m > 1";

        /*
         * Use the fast-powering algorithm as previously discussed in class,
         * with the additional feature that every multiplication is followed
         * immediately by "reducing the result modulo m"
         */
        NaturalNumber one = new NaturalNumber2(1);
        NaturalNumber two = new NaturalNumber2(2);
        NaturalNumber nTemp = new NaturalNumber2(n);
        NaturalNumber pTemp = new NaturalNumber2(p);

        if (p.isZero()) {
            n.copyFrom(one);
        } else {
            pTemp.divide(two);
            powerMod(n, pTemp, m);
            n.multiply(new NaturalNumber2(n));
            if (!isEven(p)) {
                n.multiply(nTemp);
            }
            n.transferFrom(n.divide(m));
        }
    }

    /**
     * Reports whether w is a "witness" that n is composite, in
```

```
the sense that
     * either it is a square root of 1 (mod n), or it fails to satisfy the
     * criterion for primality from Fermat's theorem.
     *
     * @param w
     *            witness candidate
     * @param n
     *            number being checked
     * @return true iff w is a "witness" that n is composite
     * @requires n > 2 and 1 < w < n - 1
     * @ensures <pre>
     * isWitnessToCompositeness =
     *     (w ^ 2 mod n = 1)  or  (w ^ (n-1) mod n /= 1)
     * </pre>
     */
    public static boolean isWitnessToCompositeness(NaturalNumber w,
            NaturalNumber n) {
        assert n.compareTo(new NaturalNumber2(2)) > 0 : "Violation of: n > 2";
        assert (new NaturalNumber2(1)).compareTo(w) < 0 : "Violation of: 1 < w";
        n.decrement();
        assert w.compareTo(n) < 0 : "Violation of: w < n - 1";
        n.increment();

        // TODO - fill in body
        boolean witness = false;
        NaturalNumber two = new NaturalNumber2(2);
        NaturalNumber one = new NaturalNumber2(1);
        NaturalNumber nMinusOne = new NaturalNumber2(n);
        NaturalNumber wTemp1 = new NaturalNumber2(w);
        NaturalNumber wTemp2 = new NaturalNumber2(w);
        nMinusOne.decrement();

        powerMod(wTemp1, two, n);
        powerMod(wTemp2, nMinusOne, n);

        if (wTemp1.compareTo(one) == 0 || wTemp2.compareTo(one) != 0) {
            witness = true;
        }

        return witness;
    }

    /**
     * Reports whether n is a prime; may be wrong with "low" probability.
     *
     * @param n
     *            number to be checked
     * @return true means n is very likely prime; false means n is definitely
     *         composite
     * @requires n > 1
     * @ensures <pre>
     * isPrime1 = [n is a prime number, with small probability of error
     *         if it is reported to be prime, and no chance of error if it is
     *         reported to be composite]
     * </pre>
     */
    public static boolean isPrime1(NaturalNumber n) {
        assert n.compareTo(new NaturalNumber2(1)) > 0 : "Violation of: n > 1";
        boolean isPrime;
        if (n.compareTo(new NaturalNumber2(THREE)) <= 0) {
            /*
             * 2 and 3 are primes
             */
            isPrime = true;
        } else if (isEven(n)) {
            /*
             * evens are composite
             */
            isPrime = false;
        } else {
            /*
             * odd n >= 5: simply check whether 2 is a witness that n is
             * composite (which works surprisingly well :-)
             */
            isPrime = !isWitnessToCompositeness(new NaturalNumber2(2), n);
        }
        return isPrime;
    }

    /**
     * Reports whether n is a prime; may be wrong with "low" probability.
     *
     * @param n
     *            number to be checked
     * @return true means n is very likely prime; false means n is definitely
     *         composite
     * @requires n > 1
     * @ensures <pre>
     * isPrime2 = [n is a prime number, with small probability of error
     *         if it is reported to be prime, and no chance of error if it is
     *         reported to be composite]
     * </pre>
     */
    public static boolean isPrime2(NaturalNumber n) {
        assert n.compareTo(new NaturalNumber2(1)) > 0 : "Violation of: n > 1";

        /*
         * Use the ability to generate random numbers (provided by the
         * randomNumber method above) to generate several
```

```
witness candidates --
         * say, 10 to 50 candidates -- guessing that n is prime only if none of
         * these candidates is a witness to n being composite (based on fact #3
         * as described in the project description); use the code for isPrime1
         * as a guide for how to do this, and pay attention to the requires
         * clause of isWitnessToCompositeness
         */

        // TODO - fill in body
        boolean prime = false;
        NaturalNumber nTemp = new NaturalNumber2(n);
        NaturalNumber one = new NaturalNumber2(1);
        NaturalNumber two = new NaturalNumber2(2);

        if (n.compareTo(new NaturalNumber2(THREE)) <= 0) {
            /*
             * 2 and 3 are primes
             */
            prime = true;
        } else if (isEven(n)) {
            /*
             * evens are composite
             */
            prime = false;
        } else {
            NaturalNumber nMinusOne = new NaturalNumber2(nTemp);
            nMinusOne.decrement();
            for (int i = 0; i <= 40; i++) {
                NaturalNumber witness = randomNumber(nTemp);
                //isWitnessToCompositeness requires: n > 2 and 1 < w < n - 1
                if (n.compareTo(two) > 0 && witness.compareTo(one) > 0
                        && witness.compareTo(nMinusOne) < 0) {
```

```
                    prime = !isWitnessToCompositeness(witness, n);
                }
            }
        }
        /*
         * This line added just to make the program compilable. Should be
         * replaced with appropriate return statement.
         */
        return prime;
    }

    /**
     * Generates a likely prime number at least as large as some given number.
     *
     * @param n
     *            minimum value of likely prime
     * @updates n
     * @requires n > 1
     * @ensures n >= #n and [n is very likely a prime number]
     */
    public static void generateNextLikelyPrime(NaturalNumber n) {
        assert n.compareTo(new NaturalNumber2(1)) > 0 : "Violation of: n > 1";

        /*
         * Use isPrime2 to check numbers, starting at n and increasing through
         * the odd numbers only (why?), until n is likely prime
         */

        // TODO - fill in body
        boolean prime = false;
        NaturalNumber two = new NaturalNumber2(2);
        //even number cannot be a prime
        if (isEven(n)) {
            n.increment();
        }
        prime = isPrime2(n);
        while (!prime) {
            n.add(two);
            prime = isPrime2(n);
        }
    }

    /**
     * Main method.
     *
     * @param args
     *            the command line arguments
     */
    public static void main(String[] args) {
        SimpleReader in = new SimpleReader1L();
        SimpleWriter out = new SimpleWriter1L();

        /*
         * Sanity check of randomNumber method -- just so everyone can see how
         * it might be "tested"
         */
        final int testValue = 17;
        final int testSamples = 100000;
        NaturalNumber test = new NaturalNumber2(testValue);
        int[] count = new int[testValue + 1];
        for (int i = 0; i < count.length; i++) {
            count[i] = 0;
        }
        for (int i = 0; i < testSamples; i++) {
            NaturalNumber rn = randomNumber(test);
            assert rn.compareTo(test) <= 0 : "Help!";
            count[rn.toInt()]++;
        }
        for (int i = 0; i < count.length; i++) {
            out.println("count[" + i + "] = " + count[i]);
        }
```

```java
        out.println("  expected value = "
                + (double) testSamples / (double) (testValue + 1));

        /*
         * Check user-supplied numbers for primality, and if a number is not
         * prime, find the next likely prime after it
         */
        while (true) {
            out.print("n = ");
            NaturalNumber n = new NaturalNumber2(in.nextLine());
            if (n.compareTo(new NaturalNumber2(2)) < 0) {
                out.println("Bye!");
                break;
            } else {
                if (isPrime1(n)) {
                    out.println(n + " is probably a prime number"
                            + " according to isPrime1.");
                } else {
                    out.println(n + " is a composite number"
                            + " according to isPrime1.");
                }
                if (isPrime2(n)) {
                    out.println(n + " is probably a prime number"
                            + " according to isPrime2.");
                } else {
                    out.println(n + " is a composite number"
                            + " according to isPrime2.");
                    generateNextLikelyPrime(n);
                    out.println("  next likely prime is " + n);
                }
            }
        }

        /*
```

```
         * Close input and output streams
         */
        in.close();
        out.close();
    }

}

```