暗号の数理レポート

- 次の 2 つの課題のいずれかをレポートとして提出すること。ただし，課題 1 は 20 点満点，課題 2 は 30 点満点とする。

課題 1 (1) 任意の自然数 m, n を入力したとき，互いに素でなければ，最大公約数を表示し，互いに素のときは

$$mp + nq = 1$$

をみたす整数 p, q を出力する Java プログラムを作成せよ。アルゴリズムは拡張ユクリッドアルゴリズムを用いること。

(2) 40 桁〜50 桁の自然数 m, n をランダムに発生させ，それに対し (1) のプログラムを適用せよ。その結果を 3 組の m, n について計算せよ。

課題 2 (1) n, b を $b < n$ となる任意の自然数とする。n が合成数であるかを b を用いて判定する Miller テストを実行する Java プログラムを作成せよ。

(2) 45 桁の自然数 n をランダムに発生させよ。また $b < n$ となる自然数 b をランダムに発生させよ。この n, b に対し (1) のプログラムを適用せよ。合成数であるという結論が得られない場合は別の b について (1) のプログラムを実行させよ。これを 5 回くり返せ。この計算結果を報告せよ。

- プログラムは情報センターの環境で動くことを確認すること。
- Java program には BigInteger クラスを使うのが簡単である。
  http://java.sun.com/j2se/1.5.0/ja/docs/ja/api/java/math/BigInteger.html 参照。
- BigInteger(int numBits, Random rnd) のより $0 \sim 2^{\mathrm{numBits}}$ の範囲の整数がランダムに生成される。例えば

```
//////////////////////////////////////////////////////
import java.math.BigInteger;
import java.util.Random;
import java.io. \uff0a ;
public class BigPrime {
  public static void main (String args[ ]){
    BigInteger p = new BigInteger ( 200, new Random( ) );
    ..............................................
  }
}
//////////////////////////////////////////////////////
```

  などとすると $0 \sim 2^{200}$ の範囲の整数 p がランダムに生成される。

- BigInteger クラスにはいろいろな constructor,method があるが，課題 1 に関しては和，積，商などの基本的なもの意外は使用してはいけない。

課題 2 については
gcd(BigInteger val)
modPow(BigInteger exponent, BigInteger m)
など計算に必要な method は使ってよいが Miller テストを行う method は使ってはいけない。

- プログラムを作成した人は
(1) 簡単なアルゴリズムの説明
(2) プログラムの使用方法
(3) 計算結果
を mail の本文にそれぞれ独立した項目として書き，プログラムを独立したファイル (そのままで実行可能な状態のファイル) として添付して crypto@math.cs.kitami-it.ac.jp まで送ること。勿論名前，学生番号も忘れずに。

- ただし「実行可能」の意味は次の通り；一連の操作が必要な場合はその手順を順に記したものでもよい。例えば実行には subdirectory XXX にある file1,file2,file3 が必要で，そのファイルが存在した場合 exec-file という名前のファイルが実行可能とする。file1,file2,file3 を例えば zip でまとめ yyy とする。unzip yyy とすると subdirectory XXX にされるように設定してあるとき，ファイルとして exec-file と yyy を添付し，リストとして,「unzip yyy; ./exec-file」と書いたものを沿えて提出。ただし unzip 等が任意の directory で実行可能でないときは full-path で書くこと。shell script が書ける人は shell script の形でもよい (というかその方が私は楽です)。

- ただしプログラム・説明文を含めて自分で書いたと思われないレポート (ネットからの copy&paste を含む) ないし他のレポートと同一と判断されるレポートは採点の対象にはならない。

- 締切は 2 月 23 日 (木) とする。