レポート提出について

- 期日: 7月25日(月)20時頃まで
- 内容: 配布プリントのレポート問題、及び授業に関連する内容で、授業内容の理解または発展的な取組みをアピールできるようなもの。
- 問1–1,1–2は、少なくとも一方を必修課題とする。
- 2節の選択課題は例である。出来れば複数に解答し提出せよ。プリントの課題例を全て提出する必要はない。また、課題例になくても関連する内容や自分で調べたり考えたりしたことがあれば、それでも良い。
- 4-574室扉のレポートポストに提出。科目名・学生番号・氏名を明記した表紙を付けよ。
- 電子メイルでの提出も可。初回の授業で配布したプリントに記載したメイルアドレス宛に、**メディアセンターの自分のアカウント**から提出すること。尚、添付ファイルで提出する際は、必ずメイル本文にプレインテキストで、学生番号・氏名・科目名・レポート内容(題目)を明記すること。

1. 必修課題

問1–1. 数理現象を利用した暗号などの高度な情報処理の方式で、**実際に使われている**ものの中から一つ選んで調べ、その特徴・性質や、何に用いられている／用いるのが適しているか、述べよ。但し、参考にした文献(書籍・ネット上の情報)があれば、それを明記すること。また、そこで用いられる基本的な概念・用語などについては、その意味・定義をきちんと述べること。

問1–2. 暗号を含めた高度な情報処理に利用されている数理アルゴリズムから一つ(以上)を選んで調べて述べよ。例えば、

- 素数判定のアルゴリズム： AKS(Agrawal-Kayal-Saxena)アルゴリズム・Miller-Rabin法・APR(Adleman-Pomerance-Rumely)法、など
- 素因数分解のアルゴリズム：二次篩法(Quadratic Sieve)・数体篩法(Number Field Sieve)・$(p-1)$法、など
- 長桁(多倍長)乗算のアルゴリズム：高速フーリエ変換(Fast Fourier Transform)
- 疑似乱数発生法：Mersenne Twister

など。但し、単なる紹介記事の引き写しではなく、数学的な説明を付けて述べること。

2. 選択課題

問2–1. 本講義内容に現れた代数系(群・環・体・加群・線型空間など)及び初等整数論などの基礎事項の中から、自分で学習したことをまとめよ。

問2–2. 本講義内容に現れた代数系及び初等整数論などの事項で、授業時に証明を省略したものについて取り上げ、証明を含めて記せ。

問2–3. 本講義内容に関連する代数系及び初等整数論などの事項を選び、証明を含めて記せ。

問2–4. 互いに素な2整数a,bに対し、$ax+by=1$となる$x,y\in\boldsymbol{Z}$を求めるアルゴリズム(Euclidの互除法拡張版)を実装せよ(プログラムを作成せよ)。

問2–5. 十進n桁の整数a,bの最大公約数$d:=\gcd(a,b)$を互除法で計算するとき、必要な割算の回数は$O(n)$であることを示し、O-constantを適切に評価せよ。(即ち、或る定数$C>0$が存在してCn回以内で済むことを示し、Cが実際にはどの程度小さく取れるか評価せよ。)

問2–6. $e=e_0+e_1\cdot 2+e_2\cdot 2^2+\cdots+e_k\cdot 2^k$ $(e_i=0,1)$とする。$m^e \bmod N$を高速に計算するアルゴリズムを記述し、何回の掛算およびNで割った余りの計算で行なえるか考察せよ。また、そのアルゴリズムを実装せよ。

問2–7. RSA暗号の公開鍵(N,e)から秘密鍵dが判れば、十分な確率で高速にNの素因数分解$N=pq$が得られる。その方法を述べよ。

問2–8. $N\times N$行列の行列式を求める計算の計算量は、Nについて如何程か。但し、各成分の大きさについては考慮する必要はなく、加算・乗算の回数を数えれば良い。(勿論、各成分の大きさも考慮しても良い。)