レポート課題 (の主な例・続き) (7/17 配布)

9. 暗号理論 (公開鍵暗号)・計算量の理論

問 9–1. 次の文字列は、Caesar 暗号 (各文字を一斉に鍵の値だけ alphabet 順にずらす) で暗号化した文字列である (全て小文字で、空白はそのまま)。鍵および平文を推測せよ。

```
phq dqg zrphq iru rwkhuv zlwk rwkhuv
```

問 9–2. 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 9–3. 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 9–4. $e = e_0 + e_1 \cdot 2 + e_2 \cdot 2^2 + \cdots + e_k \cdot 2^k$ $(e_i = 0, 1)$ とする。

(1) $m^e \bmod N$ 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。

(2) そのアルゴリズムを実装せよ。

問 9–5. k bit の数の乗算および割った余りを求める計算が $O(k^2)$ で行なえるとする。p, q を k bit の相異なる素数とし、$N = pq$ とおく。RSA 暗号の復号には、$M = C^d \bmod N$ を計算する必要があるが、これについて次のような高速化の工夫がある。

(1) $M_p := C^d \bmod p,\ M_q := C^d \bmod q$ を計算する。

(2) 中国式剰余定理により $M \equiv M_p \pmod p, M \equiv M_q \pmod q$ を解いて、$M \bmod N$ を求める。

この方法の計算量を、単純に $M = C^d \bmod N$ を計算する方法と比較せよ。(冪の計算には勿論前問の高速計算法を用いるものとする。)

問 9–6. 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 9–7. 素因数分解のアルゴリズムの二次篩法 (Quadratic Sieve) について調べよ。(他のアルゴリズムでも良いが、これが原理が一番簡単。)

問 9–8. $N \times N$ 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。)

期末試験について

- 日時: 7 月 24 日 (木) 9:15〜10:45
- 教室: 9-252 教室
- 内容: 7/17 までに講義した範囲

レポート提出について

- 期日: 8 月 4 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 5–1 は ((1)〜(4) のうち 1 つ以上を) 必修課題とする。
- 問 6–1 は、数学領域以外の理工学専攻の受講者のみ評価対象とする。
- 7 節以降の問題は、全部で 3 つ程度以上を目安に提出せよ。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。
- 授業時に手渡し、または 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ること。
- 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。