Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 8
- Proposed Solution -

Friday, June 15, 2018

Solution of Problem 1

(Multiplicative property of $\phi(n)$) Consider the set $\mathbb{Z}_{mn} = \{1, \dots, mn\}$. If $x \in \mathbb{Z}^*_{mn}$ then $\gcd(x, m) = \gcd(x, n) = 1$. The members of $\mathbb{Z}_{mn}$ can be written as $am+b$ for $a \in \{0, 1, \dots, n-1\}$ and $b \in \{1, \dots, m\}$ namely:

$$\begin{array}{cccc}
0 \times m + 1 & 0 \times m + 1 & \dots & 0 \times m + m \\
1 \times m + 1 & 1 \times m + 1 & \dots & 1 \times m + m \\
\vdots & \vdots & \ddots & \vdots \\
(n-1) \times m + 1 & (n-1) \times m + 1 & \dots & (n-1) \times m + m
\end{array}$$

For each $b_i \in \mathbb{Z}^*_m$, $am + b_i$ is also relatively prime with respect to m for $a \in \{0, 1, \dots, n-1\}$. Hence in each row of the table above there are $\phi(m)$ numbers relatively prime with respect to m. These numbers correspond to the columns $b_i \in \mathbb{Z}^*_m$ of the table above.

Now consider the column $am + b_i$ for $a \in \{0, 1, \dots, n-1\}$. Since $\gcd(m, n) = 1$, all $am + b_i$'s are n different numbers modulo n among which only $\phi(n)$ are relatively prime with respect to n. Therefore you have $\phi(m)$ columns and in each column $\phi(n)$ elements that are both relatively prime with respect to m and n. Therefore there are $\phi(m)\phi(n)$ numbers relatively prime to mn. Hence:

$$\phi(mn) = \phi(m)\phi(n).$$

Solution of Problem 2

Consider the set $K_{n-1} := \{a \in \mathbb{Z}_n \mid a^{n-1} \equiv 1 \pmod{n}\}$. It holds that $K_{n-1} \subseteq Z^*_n$, as all $a \in K_{n-1}$ have multiplicative inverses. Furthermore K_{n-1} is a subgroup of $\mathbb{Z}^*_n$, because

- it is closed under multiplication,
- the multiplication is associative,
- $1 \in K_{n-1}$,
- the inverse of a, namely a^{n-2} is in K_{n-1}, as $(a^{n-2})^{n-1} = (a^{n-1})^{n-2} \equiv 1 \pmod{n}$.

As a is not a Carmichael number, there exists $a \in \mathbb{Z}^*_n$ such that $a \notin K_{n-1}$, so K_{n-1} is a proper subgroup of $\mathbb{Z}^*_n$. By Lagrange's theorem it holds that

$$|K_{n-1}| \text{ divides } |\mathbb{Z}^*_n|,$$

hence

$$|K_{n-1}| \leq \frac{1}{2}|\mathbb{Z}_n^*| \leq \frac{n-2}{2}.$$

Finally we conclude that

$$|\mathbb{Z}_n \setminus \{0\} \setminus K_{n-1}| \geq n-1-\frac{n-2}{2} = \frac{n}{2}.$$

Solution of Problem 3

a) Define event A : 'n composite' $\Leftrightarrow \bar{A}$: 'n prime'.
Define event B : m-fold MRPT provides 'n prime' in all m cases.
From hint: $\text{Prob}(\bar{A}) = \frac{2}{\ln(N)} \Rightarrow \text{Prob}(A) = 1 - \frac{2}{\ln(N)}$ (cf. Thm. 6.7)

Probability for the case that the MRPT fails for m times:

$$\text{Prob}(B \mid A) \leq \left(\frac{1}{4}\right)^m$$

Probability of the MRPT verifying an actual prime is:

$$\text{Prob}(B \mid \bar{A}) = 1$$

Probability of the MRPT wrongly verifying a composite n as prime after m tests is:

$$\begin{aligned} p &= \text{Prob}(A \mid B) \\ &= \frac{\text{Prob}(B \mid A) \cdot \text{Prob}(A)}{\text{Prob}(B)} \\ &= \frac{\text{Prob}(B \mid A) \cdot \text{Prob}(A)}{\text{Prob}(B \mid A) \cdot \text{Prob}(A) + \text{Prob}(B \mid \bar{A}) \cdot \text{Prob}(\bar{A})} \\ &\leq \frac{(\frac{1}{4})^m(1-\frac{2}{\ln(N)})}{(\frac{1}{4})^m(1-\frac{2}{\ln(N)}) + 1 \cdot \frac{2}{\ln(N)}} \\ &= \frac{\ln(N)-2}{\ln(N)-2+2^{2m+1}} \end{aligned}$$

b) Note that the above function $f(x) = \frac{x}{x+a}$ is monotonically increasing for $x \in \mathbb{R}$, $a > 0$, as its derivative is $f'(x) = \frac{a}{(x+a)^2} > 0$. Let $x = \ln(N) - 2$, and $N = 2^{512}$.
Resolve the inequality w.r.t. m:

$$\begin{aligned} \frac{x}{x+2^{2m+1}} &< \frac{1}{1000} \\ \Leftrightarrow 2^{2m+1} &> 999x \\ \Leftrightarrow m &> \tfrac{1}{2}(\log_2(999x) - 1) \\ \Leftrightarrow m &> \tfrac{1}{2}(\log_2(999(512\ln(2)-2)) - 1) \\ \Leftrightarrow m &> 8.714. \end{aligned}$$

$m = 9$ repetitions are needed to ensure that the error probability stays below $p = \frac{1}{1000}$ for $N = 2^{512}$.