Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 8
- Proposed Solution -

Friday, June 17, 2016

Solution of Problem 1

Proof by contradiction:

Assume there is only a finite number of n primes $p_1, p_2, ..., p_n$ (sorted in an ascending list). This implies that all other integers (except the p_i) greater than one are supposed to be composite by assumption.

Construct a number composed of the product of *all* primes plus one:

$$P = \prod_{i=1}^{n} p_i + 1 \tag{1}$$

$P > p_n$ and assumed to be composite. As P is composite, it must have at least one prime factor p with $p > 1$ so that $p|P$. As p is assumed to be prime, it holds $p| \prod_{i=1}^{n} p_i$.

Let us reformulate the above equation (1) to:

$$P - \prod_{i=1}^{n} p_i = 1 \tag{2}$$

Since both $p|P$ and $p| \prod_{i=1}^{n} p_i$ holds, we obtain $p|(P - \prod_{i=1}^{n} p_i)$. However, $P - \prod_{i=1}^{n} p_i = 1$. It is obvious that no $p > 1$ divides 1. $\lightning$

As a result there is at least one other prime $p = p_{n+1}$ greater than p_n. By induction this continues for $n \to n+1$, so that there are infinitely many primes. ■

Solution of Problem 2

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:

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

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

Solution of Problem 3

a) Let n be odd and composite. The problem is modelled by a geometric distributed random variable X with:

- Probability of a single test stating 'n is prime' although n is composite is p ($\Rightarrow 1-p$ for 'n is composite')
- Probability that after exactly $M \in \mathbb{N}$ tests, it correctly states 'p is composite':

$$\text{Prob}(X = M) = p^{M-1}(1-p)$$

b) The expected value of a geometrically distributed random variable is:

$$\mathsf{E}(X) = \sum_{M=1}^{\infty} M p^{M-1}(1-p) = (1-p)\frac{p}{(1-p)^2} = \frac{p}{1-p},$$

Note that with the geometric series $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$, we can compute its derivative w.r.t. x, and obtain $\sum_{n=1}^{\infty} n x^{n-1} = \frac{x}{(1-x)^2}$, for $|x| < 1$.

For the given parameter $p = \frac{1}{4}$, the expected value for the number of tests stating that a composite n is indeed composite is:

$$\mathsf{E}(X) = \frac{p}{1-p} = \frac{1/4}{1-1/4} = \frac{1/4}{3/4} = \frac{1}{3}$$

Solution of Problem 4

a) By the Miller-Rabin Primality Test it will be proven that 341 is composite.
Write $n = 341 = 1 + 85 \cdot 2^2 = 1 + q \cdot 2^k$.

Algorithm 1 Miller-Rabin Primality Test (MRPT)

Write $n = 1 + q2^k, q$ odd
Choose $a \in \{2, \dots, n-1\}$ uniformly distributed at random
$y \leftarrow a^q \mod n$
if $(y = 1)$ OR $(y = n - 1)$ **then**
  return "n prime"
end if
for $(i \leftarrow 1; i < k; i{+}{+})$ **do**
  $y \leftarrow y^2 \mod n$
  if $(y = n - 1)$ **then**
    return "n prime"
  end if
end for
return "n composite"

Choose $a = 2$.
Calculate $a^q \mod n$, i.e., $2^{85} \mod 341$.
Note that $2^{10} = 1024 = 3 \cdot 341 + 1 \equiv 1 \mod 341$.
It follows $2^{85} = (\underbrace{2^{10}}_{\equiv 1})^8 \cdot \underbrace{2^5}_{=32} \equiv 32 \mod 341$.
Alternatively, $2^{85} \mod 341$ is calculated by Square and Multiply, see below. As $y = 32 \notin \{1, n-1\}$ the for-loop starts with $i = 1$.
$y^2 = 32^2 = (2^5)^2 = 2^{10} \equiv 1 \mod 341$, see above.
Furthermore, $y = 1 \neq 340 \mod 341$.
As $i = 2 = k = 2$ the for-loop terminates and n is stated as composite, which is a reliable result.

b) A number n is decomposed according to MRPT as $n = 1 + q\,2^k$. It follows that MRPT has at most k squarings. The worst case occurs, if $q = 1$, then $n = 1 + 2^k \Leftrightarrow k = \log_2(n-1)$.
With n having 300 digits it follows: $n < 10^{301} = (\underbrace{10^3}_{<2^{10}})^{100} \cdot \underbrace{10}_{<2^4} < 2^{1004} \Rightarrow k \leq 1004$.
Consequently, less than 1004 squarings are needed. ($k \approx 999.9$)

Note, evaluating $a^q \mod n$ with Square and Multiply takes t squarings. But as $2^t \leq q$ holds, the worst case is reached, for equality which means $t = 0$, i.e., $q = 1$, as otherwise q would be not odd.

Determining $2^{85} \mod 341$ by Square and Multiply.
It holds $a = 2$, $x = 85 = (1010101)_2$, i.e., $t = 6$.
The following tabular denotes the evaluation of the Square and Multiply algorithm. The table is initialized in the first line with $i = t = 6$ and $y = 1$. There are $t + 1$ lines numbered from t down to 0. The binary representation of $x = (x_t. \dots .x_0)$ is given in column two. Using those values the columns four and five are evaluated row by row. For each row the y value is taken from the last column of the row above. The final value in the fifth column is the result of $a^x \mod n$.

Algorithm 2 Square and multiply

Require: $x = (x_t, \dots, x_0) \in \mathbb{N}, a \in \mathbb{N}$
Ensure: $a^x \mod n$

$y \leftarrow a$
for $(i = t-1, i \geq 0, i\text{--})$ **do**
    $y \leftarrow y^2 \mod n$
    if $(x_i = 1)$ **then**
        $y \leftarrow y \cdot a \mod n$
    end if
end for
return y

i	x_i	y	$y^2 \mod n$	$y^2(1 + x_i \cdot (a-1)) \mod n$
6	1	1	1	2
5	0	2	4	4
4	1	4	16	32
3	0	32	$1024 \equiv 1 \mod 341$	1
2	1	1	1	2
1	0	2	4	4
0	1	4	16	32

The solution is $2^{85} \equiv 32 \mod 341$.