Problem Set 3 (Solutions)

1. Suppose \( \Theta = \frac{P}{Q} \). Put \( \epsilon := \frac{1}{Q} \).

By hypothesis, \( \exists \ M \in \mathbb{N} \) s.t. \( m \geq M \implies 0 < \left| \frac{P}{Q} - \frac{a_m}{l_m} \right| < \frac{1}{q_{2m}} \implies 0 < \left| p_{2m} - 2a_m \right| < 1 \)

which is impossible.

2. \( \Theta := \epsilon, \ a_m := \frac{m!}{m!} \), \( b_m := \sum_{k=0}^{m} \frac{m!}{k!} \). Put \( f(t) = e^t \).

Then \( f(1) = \frac{P_m(1) + R_m(1)}{b_m} = \frac{b_m}{x_m} + \sum_{m+1}^{1} \frac{f^{(m+1)}(t)}{m!} \) (remainder).

\[
\Rightarrow e - \frac{b_m}{a_m} = \int_0^1 \frac{e^t}{m!} (1-t)^m dt < \frac{3}{(m+1)!} = \frac{3^{(m+1)}}{a_m}.
\]

So given \( \epsilon > 0 \), taking \( M \) so that \( \frac{3}{m+1} < \epsilon \) shows the condition of Exercise 1 holds. Therefore \( \epsilon \notin A \).

3. First, note \( \frac{\log p_{i+1} - \log p_i}{p_{i+1} - p_i} \to 0 \) (here \( p_i \) is the \( i \)-th prime).

Since \( \frac{\log p_{i+1} - \log p_i}{p_{i+1} - p_i} \sim \frac{1}{p_i} \) (derivative of \( \log x \) is \( \frac{1}{x} \)) and \( \pi(x) \approx \frac{x}{\log x} \).

Henceforth, \( \lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1 \implies \lim_{x \to \infty} \frac{\Delta \pi(x)}{\Delta x} = 1 \)

\[
\Rightarrow 1 = \lim_{i \to \infty} \frac{\pi(p_{i+1}) \log p_{i+1} - \pi(p_i) \log p_i}{p_{i+1} - p_i}.
\]
\[
\lim_{i \to a} \frac{\log p_i}{\log p_i} = \lim_{i \to a} \left\{ \frac{\log p_i - \log p_i}{p_i - p_i} + \frac{\log p_i}{p_i - p_i} \right\} = \lim_{i \to a} \frac{\log p_i}{p_i - p_i} \to 0
\]

Of course, this isn't rigorous, but suggests the difference \( p_{i+1} - p_i \) tends to \( \log p_i \).

4. \( \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2, \phi(7) = 6, \phi(8) = 4, \phi(9) = 6, \phi(10) = 4, \phi(11) = 10, \phi(12) = 4 \).

5. By Little Fermat, \( n^{12} - n \) is divisible by any prime \( p \) for which \( p-1 \) divides \( 12 \) \( \Rightarrow n^{12} \equiv (n^{p-1})^{12} \equiv 1 \equiv n \) \( \pmod{p} \).

For \( p = 2, 3, 5, 7, 13 \), \( p-1 \) divides \( 12 \).

6. \( m = 2n + 1, \ a = \begin{cases} 2k + 1 & \Rightarrow 2m + a^2 = \begin{cases} 4(n+k^2+k) + 3 & \equiv 3 \\ 4(n+k^2) + 2 & \equiv 2 \end{cases} \end{cases} \).

But the squares \( \pmod{4} \) are \( 0 \) or \( 1 \).

7. See next page.

8. The idea here for (ii) is to use that \( a^{p-2} \cdot a = a^{p-1} \equiv 1 \pmod{p} \) \( \Rightarrow a^{p-2} \) is an inverse for \( a \pmod{p} \). I'll just say that the answers are:

- \( 11^{-1} \equiv -17 \equiv 30 \pmod{47} \) \( \pmod{47} \)

and

- \( 345^{-1} \equiv 114 \pmod{587} \)
Algorithm: Given \( N, g, A \in \mathbb{N} \),

1. Set \( a := g, \quad b := 1 \)
2. If \( A = 0 \), go to Step 6
3. If \( A \equiv 1 \pmod{2} \), set \( b := b \cdot a \)
4. Set \( a := a^2 \), \( A := \lceil A/2 \rceil \)
5. Go to Step 2
6. Output \( b \).

Proposition: The output is \( g^A \pmod{N} \).

Proof: is by induction on \( A \)

\((A = 0)\): \( g^0 = 1 \) (ok)

Inductive Step: Case 1 \((A \equiv 0)\): Running the algorithm is equivalent to replacing \( \{ \frac{g}{A} \} \) by \( g^2 \), and running the algorithm. By inductive assumption, output \( = (g^2)^{A/2} = g^A \pmod{N} \).

Case 2 \((A \equiv 1)\): Running the algorithm is equivalent to:

- Replacing \( \{ g \} \) by \( g^2 \),
- \( \{ A \} \) by \( A/2 \),
- Running the algorithm,
- Multiplying the output by \( g \).

The output, using the inductive assumption, is \( g \cdot (g^2)^{A/2} = g \cdot g^{A-1} = g^A \pmod{N} \).