Appendix 4: Number theory

Hongyuan Sun*

July 27, 2020

A4.1 Fundamentals

A4.2 Modular arithmetic and Euclid's algorithm

A4.3 Reduction of factoriing to order-finding

A4.4 Continued fraction

Exercise A4.18

$$x = \frac{19}{17} = [1, 8, 2] \tag{AE4.18-1}$$

$$x = \frac{77}{65} = [1, 5, 2, 2, 2] \tag{AE4.18-2}$$

Exercise A4.19

Proof.

$$\because \begin{cases} [a_0] = a_0 = \frac{p_0}{q_0} \\ [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{p_1}{q_1} \end{cases} \tag{AE4.19-1}$$

$$\therefore \begin{cases} p_0 = a_0 \\ q_0 = 1 \end{cases} \quad \begin{cases} p_1 = a_0 a_1 + 1 \\ q_1 = a_1 \end{cases} \tag{AE4.19-2}$$

$$\therefore q_1 p_0 - p_1 q_0 = a_0 a_1 - (a_0 a_1 + 1) = -1$$

If $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ for $n = k$, then with equations (AE4.42),(AE4.43), we can get

$$q_{k+1} p_k - p_{k+1} q_k = (a_{k+1} q_k + q_{k-1}) p_k - (a_{k+1} p_k + p_{k-1}) q_k \tag{AE4.19-3}$$

$$= a_{k+1}(q_k p_k - p_k q_k) + q_{k-1} p_k - p_{k-1} q_k \tag{AE4.19-4}$$

$$= -(-1)^k = (-1)^{k+1} \tag{AE4.19-5}$$

So $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ for $n = k+1$, using inductive reasoning we can prove that this statement is true for $n \geqslant 1$. □

Problem 4.1(Prime number estimate)

(1)

Proof.

$$\log \binom{2n}{n} = \log \frac{\prod_{i=0}^{n-1}(2n-i)}{\prod_{i=0}^{n-1}(n-i)} \tag{AP4.1-1}$$

$$= \log \prod_{i=0}^{n-1} \frac{2n-i}{n-i} \tag{AP4.1-2}$$

$$\geqslant \log 2^n \tag{AP4.1-3}$$

$$= n$$

□

*E-mail:LargeDumpling@foxmail.com

(2)

(3)

Proof.

$$
\begin{aligned}
\because n &\leqslant \log \binom{2n}{n} && \text{(AP4.1-4)}\\
&\leqslant \sum_{p \leqslant 2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log p && \text{(AP4.1-5)}\\
&\leqslant \sum_{p \leqslant 2n} \log(2n) && \text{(AP4.1-6)}\\
&= \pi(2n)\log(2n) && \text{(AP4.1-7)}
\end{aligned}
$$

$$
\therefore \pi(2n) \geqslant \frac{n}{\log(2n)} \qquad \square
$$