1. (String Matching) 

(a) (Rabin-Karp algorithm) First create a list of 2 digit numbers \( n \) where \( \text{val}(n) = 5 \). The list is 05 12 19 26 33 40 47 54 61 68 75 82 89 96. Then create the desired string as follows: start with any digit \( x \), find a \( y \) so that \( xy \) is in the list, and repeat this step with \( x \) set to \( y \). The result is not unique, because there is sometime more than one choice for \( y \). Starting with 1, I get 1 2 6 8 9 6 1 9.

(b) Proof is by induction on \( i \).

- \( i = 1 \): We have to show that \( c(ab)^n a = (ab)^{n-1} a \), for \( n \geq 1 \). This follows from: (1) \( (ab)^{n-1} a \) is both a prefix and a suffix of \((ab)^n a\), and (2) the only longer proper prefix of \((ab)^n a\) is \((ab)^n\), which is not a suffix.

- \( i + 1 \): Assume \( c^i((ab)^n a) = (ab)^{n-i} a \), where \( i < n \). We show that \( c_{i+1}(ab)^n a = (ab)^{n-i-1} a \).
  \[
  c^{i+1}(ab)^n a = \{\text{definition of } c^{i+1}\} \\
  c(c^i((ab)^n a)) = \{\text{induction hypothesis}\} \\
  c((ab)^{n-i} a) = \{\text{from the first proof}\} \\
  (ab)^{n-i-1} a
  \]

(c) Yes. Suppose \( v = "ab" \) and \( v' = "aba" \). Then \( c(v) = \epsilon \), and \( u \) has been set to \( c(v) \), i.e., \( \epsilon \), before this portion of the code is executed. Because \( p[v] \) and \( p[\bar{v}] \) are both "a", \( c(v') \) will be set "a".

(d) (KMP Algorithm)

\[
\begin{array}{c|cccccccccccc}
 l & index & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
\hline
 text & a & b & a & b & a & b & a & b & a & b & a & b \\
 0 & pattern & a & b & a & b & a & b & a & b & a & b & a & b \\
 2 & pattern & a & b & a & b & - & - \\
 4 & pattern & a & b & - & - & - & - \\
 5 & pattern & a & b & a & - & - & - \\
 7 & pattern & a & b & - & - & - & - \\
 8 & pattern & a & b & a & b & - & - \\
\end{array}
\]

It is possible to terminate the algorithm when \( l = 7 \), because the text cannot possibly match the pattern.
2. (Data Parallel Programming)

(a) We show that for \( n \geq 1 \), \( \text{rev}(f \ n) = (f \ n) \). The required result follows because

\[
\begin{align*}
f(n + 1) & \quad \{\text{definition of } f\} \\
(f n) \ | \ \text{rev}(f n) & \quad \{\text{rev}(f n) = (f n)\} \\
(f n) \ | \ (f n) & \quad \{\text{rev}(f n) = (f n)\}
\end{align*}
\]

The proof is by induction on \( n \).

- \( n = 1 \): We show \( \text{rev}(f 1) = (f 1) \). From the definition of \( f \), 
  \( (f 1) = \langle 0 \ 1 \ 1 \ 0 \rangle \). And from the definition of \( \text{rev} \), \( \text{rev}(f 1) = \langle 0 \ 1 \ 1 \ 0 \rangle \). Hence \( \text{rev}(f 1) = (f 1) \).

- \( n + 1 \): Assume by induction hypothesis that \( \text{rev}(f n) = (f n) \). Then,

\[
\begin{align*}
\text{rev}(f(n + 1)) & \quad \{\text{definition of } f\} \\
\text{rev}((f n) \ | \ \text{rev}(f n)) & \quad \{\text{induction hypothesis applied to the second term}\} \\
\text{rev}((f n) \ | \ (f n)) & \quad \{\text{definition of } \text{rev}\} \\
\text{rev}(f n) \ | \ \text{rev}(f n) & \quad \{\text{induction hypothesis applied to the first term}\} \\
(f n) \ | \ \text{rev}(f n) & \quad \{\text{definition of } f\} \\
f(n + 1) & \quad \{\text{definition of } f\}
\end{align*}
\]

(b) i. \((u \sim r) \land (v \sim s)\)

ii. \(gr\ u = u \sim (rr\ u)\), where \(rr\) is right-rotate.

iii. \(gr(u \triangledown v)\)

\[
\begin{align*}
gr(u \triangledown v) & \quad \{\text{definition of } gr\} \\
(u \triangledown v) \sim rr(u \triangledown v) & \quad \{\text{definition of } rr\} \\
(u \triangledown v) \sim ((rr\ v) \triangledown u) & \quad \{\text{from (i)}\} \\
(u \sim (rr\ v)) \land (v \sim u) & \quad \{\text{rewrite the second term}\} \\
(u \sim (rr\ v)) \land (u \sim v) & \quad \{\text{rewrite the second term}\}
\end{align*}
\]