Discrete Mathematics and Applications

Moshe Rosenfeld

Hanoi 2010 moishe@u.washington.edu

1 Assignment No. 9: scheduling, recurrence relations, prime numbers

Due: Wednesday, 15 Dec.

Please submit your answer in a neat, readable properly organized format.

1. How much money will you have to pay Mr. Nguyen to complete your Xe May if the list of tools you need is:

 $\begin{array}{l} 11, \, 5, \, 4, \, 12, \, 15, \, 8, \, 8, \, 16, \, 3, \, 1, \, 2, \, 6, \, 1, \, 1, \, 19, \, 7, \, 15, \, 6, \, 19, \, 9, \, 5, \, 6, \\ 18, \, 15, \, 14, \, 16, \, 18, \, 20, \, 9, \, 16, \, 5, \, 6, \, 14, \, 16, \, 13, \, 4, \, 4, \, 6, \, 17, \, 4, \, 7, \, 11, \\ 19, \, 18, \, 5, \, 2, \, 8, \, 7, \, 20, \, 14, \, 17, \, 17, \, 4, \, 15, \, 2, \, 4, \, 9, \, 17, \, 19, \, 5, \, 4, \, 14, \, 9, \\ 18, \, 19, \, 2, \, 20, \, 15, \, 7, \, 19, \, 11, \, 12, \, 1, \, 9, \, 16, \, 3, \, 1, \, 4, \, 14, \, 7, \, 18, \, 12, \, 7, \\ 17, \, 1, \, 6, \, 3, \, 17, \, 10, \, 17, \, 7, \, 6, \, 9, \, 15, \, 16, \, 8, \, 9, \, 13, \, 9, \, 19 \end{array}$

- 2. Building companies submit requests to the "Hanoi Big Crane" company. Each request specifies the time the crane is needed and for how long. For example, a (30, 9) request means the crane is needed on the 30-th day for 9 days. You are asked to produce a schedule that will satisfy the largest number of requests to maximize the company's profit. Your friend suggests the following three alternatives:
 - (a) Always select an available request that starts earliest.
 - (b) Among the current requests, select the one that requires the least amount of time.
 - (c) Among the current requests select the one with the fewest conflicts (other requests with overlap times).

For each asuggestion construct an example that shows that it does not produce an optimal schedule.

3. Jobs are submitted for processing on a single resource. Once a job starts it cannot be interrupted. Each job submits two numbers: p_i, d_i where p_i is the processing time and d_i the deadline when it is needed. It is suggested that the following selection will minimize the number of late jobs.

Sort the jobs by processing time. Select the one with the shortest processing time, remove from the list all jobs that cannot be completed on time because of the current selection.

Does this guaranteed an optimal selection?

- 4. Find the solution to the following recurrence relations:
 - (a) Find all solutions to: $a_n = 5a_{n-1} 6a_{n-2} + 2^n + 3n_{n-2}$
 - (b) $a_n = 3a_{n-1} 3a_{n-2} + a_{n-3}, a_0 = 1, a_1 = 0, a_2 = 1$
 - (c) General solution for $a_n = a_{n-1} a_{n-2}$
 - (d) Solve: $a_n = 4a_{n-1} 4a_{n-2} + 2^n$, $a_0 = a_1 = 1$
- 5. Show that $D_n = nD_{n-1} + (-1)^n$ where D_n is the number of derangements.

1.1 Numbers, prime and not so prime

For the numerical calculations you will need to use a math software such as MATLAB, Sage, Mathematica, Maple etc. The following functions are either built-in the package you are using or you will have to implement them.

1. $\operatorname{xgcd}(a,b)$ returns three integers x, y, m such that: gcd(a,b) = m = xa + yb.

2. pmod(a, b, n) or modexp(a, b, n) returns $a^b \mod n$. A sample coding of this function can be found in the document number heavy-crypto.pdf.

- 1. Let n = your nine digit phone number. Let p be the smallest prime of the form 4k + 1 greater than n^{10} .
 - (a) Check whether n is a quadratic residue mod p.
 - (b) If it is, find its square-root mod p. If not, try n + 1, n + 2, ... until you identify a number which has a square root, then find it.
- 2. Select two prime numbers p, q each about 50 digits long. Make sure that $p, q, \mod 4 = 3$. Let k = p * q. Randomly select 3 numbers a_1, a_2, a_3 . For each number calculate all square roots of $a_i^2 \mod k$.
- 3. $p \cdot q = 11446899894264617414731822632826935351396699011$ 738444410675096067716991703269620363366611171741767

$$\begin{split} \phi(p \cdot q) &= 11446899894264617414731822632826935351396698870\\ 796710116539819311771464406220868402170157896702000 \end{split}$$

Find p and q.

4. Prove that $gcd(2^n - 1, 2^m - 1) = 2^{gcd(n,m)} - 1$ n, m positive integers.