Chris Wong SID 860923521

CS 111 ASSIGNMENT Homework 2

due 4/26/2011

Problem 1: Let $_k = \{1, 2, ..., k\}$ be the set of natural numbers between 1 and k, where k is some natural number. For a natural number x, by $F(x)$ we denote the set of its prime factors.

(a) We define relation $\bowtie$ on $_k$ as follows: $x \bowtie y$ if and only if $F(x) = F(y)$. List all equivalence classes of $\bowtie$ for $_{30}$.

(b) Now define relation $\trianglelefteq$ on the equivalence classes of $\bowtie$: $[x] \trianglelefteq [y]$ if and only if $F(x) \subseteq F(y)$.
Prove that $\trianglelefteq$ is a partial order. Also, draw the Hasse diagram of $\trianglelefteq$ for $_{14}$. For example, the reverse page shows the Hasse diagram of $\trianglelefteq$ for $_{10}$.

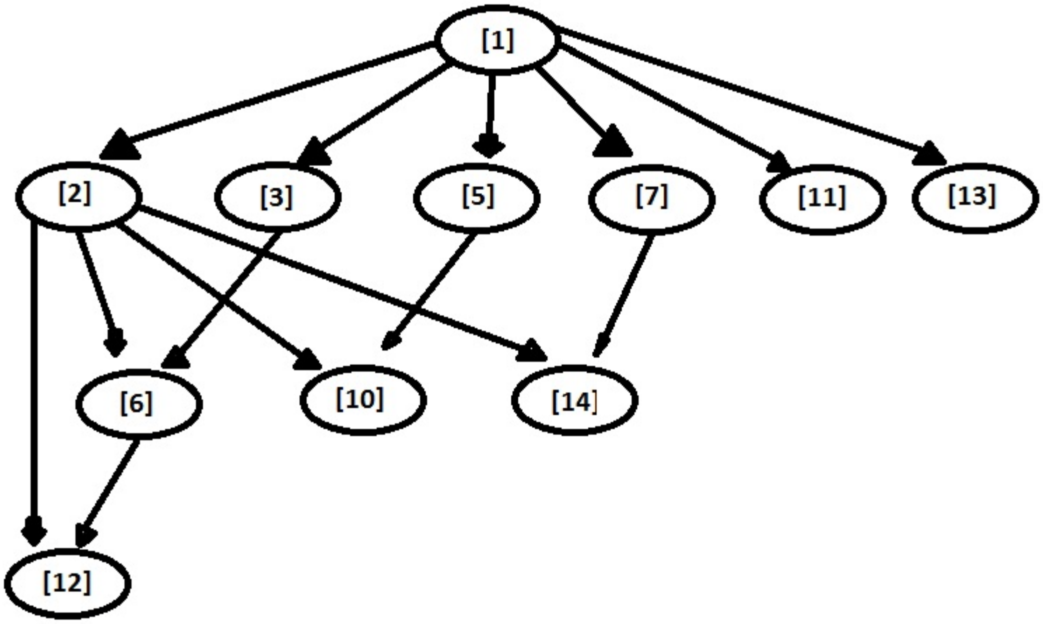
Solution 1:
a) equivalence classes of $\bowtie$ for $_{30}$.
$[1] = \{1\}$, $[2] = \{2, 4, 8, 16\}$, $[3] = \{3, 9, 27\}$,
$[5] = \{5\}$, $[6] = \{6\}$, $[7] = \{7\}$,
$[10] = \{10\}$, $[11] = \{11\}$, $[12] = \{12\}$,
$[13] = \{13\}$, $[14] = \{14\}$, $[15] = \{15\}$,
$[17] = \{17\}$, $[18] = \{18\}$, $[19] = \{19\}$,
$[20] = \{20\}$, $[21] = \{21\}$, $[22] = \{22\}$,
$[23] = \{23\}$, $[24] = \{24\}$, $[26] = \{26\}$,
$[28] = \{28\}$, $[29] = \{29\}$, $[30] = \{30\}$,

b) $[x]R[y] \Leftrightarrow f(x) \leq f(y)$
$[1]R[2] \rightarrow empty \leq 2, 4, 8, 16 \rightarrow true$
$[2]R[5] \rightarrow 2, 4, 8, 16 \leq 5 \rightarrow false$
$[75]R[15], [15]R[75] \rightarrow 15, 45, 75 \rightarrow [15] = [75]$
$[30]R[90], [90]R[30] \rightarrow 30, 60, 90 \rightarrow [30] = 90$
Thus, it is anti-symmetric is on the equivialence classes.

$[x]R[x]$
$\rightarrow [1]R[1] \rightarrow empty \leq empty \rightarrow true$
$\rightarrow [2]R[2] \rightarrow 2, 4, 8, 16 \leq 2, 4, 8, 16 \rightarrow true$
$\rightarrow [x] \leq [x]$
Thus, it is reflexive

$[x]R[y], [y]R[z], [x]R[z]$
$\rightarrow [1]R[2], [2]R[6], [1]R[6] \rightarrow [1] \leq [6] \rightarrow true$
$\rightarrow [1]R[5], [5]R[10], [1]R[10] \rightarrow [1] \leq [10] \rightarrow true$
$\rightarrow [3]R[6], [6]R[12], [3]R[12] \rightarrow [3] \leq [12] \rightarrow true$
Thus, it is transitive con't $\rightarrow$

We can conclude that the relation is of partial order because it is anti-symmetric, reflexive, and transitive



Problem 2: In the RSA, Bob chooses $p = 11$, $q = 17$. He is considering three choices for the public exponent e: 5, 7 and 33, but he's not sure whether they are correct.

(a) Which of these three choices for e are correct? Justify your answer.

(b) Let now e be the smallest correct choice. Determine the value of the secret exponent d.

(c) Suppose Alice wants to send $M = 26$ to Bob. Determine the ciphertext C.

(d) What computation will Bob perform to decrypt C? Show the result.

In parts (b), (c), (d), you don't need to show the details of the computation (a calculator may be useful for this), but you need to explain what steps are required to obtain the result.

Solution 2:
a) n = pq = (11)(17) = 187
x = (p-1)(q-1) = (11-1)(17-1) =160
e must statisfy the following conditions:
1 < e < x, gcd(x,e) == 1, e == prime number

for 5: gcd(160,5) = 5 != 1; fails condition
for 33: 33 != prime number; fails condition
for 7: 1 < 7 < 160 is true; gcd(160,7) == 1; 7 == prime number

Since 7 statfies all the conditions and 5 33 fail at least one we can
conclude that 7 is the correct choice for 'e'
e = 7

b)smallest correct choice = 7
p = 11, q = 17, e = 7
thus n = 187 and x = 160
d = e^{-1}(mod(x)) = 7^{-1}(mod160)
7z + 160y = 1 $\rightarrow 7(23) + 160(1) \rightarrow z = d = 23$

c)m$^e(rem(n)) \rightarrow 26^7(rem(187)) \rightarrow c = 104$

$d)Ds(c) = c^d(rem(n)) \rightarrow 104^{23}(rem(187)) = 26$

Problem 3: Individual assignment, do not need to complete problem 3

Solution 3: Individual assignment, do not need to complete problem 3
