CS 255 – Homework 4

Team Members:
Ravali Koppaka(012445693)
Vincent Stowbunenko(005625269)

1. Consider the variant of the paging problem where requests come in as before, but now a request can either be for a single page or two contiguous pages. How does this affect the number of cache misses MIN makes in the worst case? How does it affect our lower bound $C_{oblR} \geq H_k$? (State any assumptions you make). How competitive is the Marker algorithm in this case? (Give a reasonable upper bound)

Solution:

Assumptions: Cache size - k, distinct pages – k + 1, no of requests – N with every request being two contiguous pages

Number of cache misses in worst case for MIN:
If every request is two contiguous pages, only $\frac{k}{2}$ pages will be in cache. For the next $\frac{k}{2}$ -1 request at least one of the page will not be requested. We evict the furthest page in the request sequence from the cache and there are $\frac{k}{2}$ misses for every k requests. So, we would have $\frac{N}{k} \times \frac{k}{2} = \frac{N}{2}$

MIN would have $\mathbf{\frac{N}{2}}$ cache misses in worst case

Lower Bound:

We split the request sequence into rounds.
MIN being the best offline algorithm has $\frac{k}{2}$ misses for every round.
For the online algorithm A, the probability that the item *A* leaves out is requested is $1/(k/2) = 2/k$. Hence, it follows that the expected number of missed per round is $2H_k$

So lower bound would be $2H_k/(k/2) = \mathbf{4H_k/k}$

Marker Algorithm (Competitiveness):

Marker Algorithm would have a $\mathbf{2H_{k/2}}$ Competitiveness.
Since we have k/2 cache locations for pages with request (two contiguous pages)
Offline algorithm would have the same miss rate of $\frac{m}{2}$ (using the same argument in slides)

The expected cost of Marker algorithm is Marker algorithm:
m requests to clean items costs Marker a miss

Of the $k/2 - m$ requests to stale items, the expected cost of each is the probability that the item is not in the cache. This is maximized when the m requests to clean items precede all the $k/2 - m$ requests to stale items.
For $1 \le i \le (k/2) - m$, the probability that the ith request to a stale item is a miss is $m/(k/2) - i + 1$. Summing over i shows that the expected cost of Marker is bounded by $m + m(Hk/2 - Hm) \le mHk/2$.

2. Use the extended Euclidean algorithm to find the multiplicative inverse of $7 \bmod 165$. Solve $8x = 6 \bmod 10$ for all solutions.

Solution:

Abbreviated Extended Euclidean to EE
EE(7,165)
EE(EE(165,7))
EE(EE(EE(7,4)))
EE(EE(EE(EE(4,3))))
EE(EE(EE(EE(EE(3,1)))))
EE(EE(EE(EE(EE(EE(1,0))))))

Each EE(a,b) returns tuple (d,x,y); d = gcd(a,b); x,y such that ax+by = d

EE(EE(EE(EE(EE(1,1,0)))))
EE(EE(EE(EE(1,0,1))))
EE(EE(EE(1,1,-1)))
EE(EE(1,-1,2))
EE(1,2,-47)
(d,x,y) = (1,-47,2)
x = -47
Multiplicative Inverse in Z_{165} = (165 – 47) = 118

Solve $8x = 6 \bmod 10$
Equation ax = bmodn is solvable iff gcd(a,n)|b
d = gcd(8, 10) = 2
2|6, So the equation is solvable

It had d = 2 solutions
$Z_{10}\langle 8 \rangle = \langle 8,6,4,2,0 \rangle$
$8*2 = 6 \bmod 10$
x = 2
period $|\langle 8 \rangle| = 5$
x = 2+5 = 7
Solution of the equation is x = {2,7}

3. Using the Chinese Remainder theorem determine a number x mod 165 that satisfies $x \bmod 3 = 2$, $x = 3 \bmod 5$, and $x = 8 \bmod 11$.

Solution:

Using Chinese Remainder theorem
n = 165
= 3*5*11 ($n_1 * n_2 * n_3$)
$m_1 = \frac{165}{3} = 55$
$m_2 = \frac{165}{5} = 33$
$m_3 = \frac{165}{11} = 15$
Using Extended Euclidean we found the multiplicative inverse of m_1, m_2, m_3
as $t_1 = 1$; $t_2 = 2$; $t_3 = 3$
$c_1 = m_1 * t_1 = 55*1 = 55$
$c_2 = m_2 * t_2 = 33*2 = 66$
$c_3 = m_3 * t_3 = 15*3 = 45$

$a_1 = 2$
$a_2 = 3$
$a_3 = 8$

$a = c_1 a_1 + c_2 a_2 + c_3 a_3$
a = 668
x = a mod 165
x = 8

4. Suppose *p*=11, *q*=13. If we choose *e*=7, what would be the RSA public and private keys? Show the result of encrypting with the private key, the message 97. Show the steps in decrypting it, to get the original number back.

Solution:

n = pq
= 11*13
= 143
e = 7
Public Key (e,n) = (7,143)

$\Psi(n) = (p - 1)(q - 1) = 120$
Using Extended Euclidean, multiplicative inverse of e (7 mod 120); d = 103

Private Key (d,n) = (103, 143)

Encryption
M = 97, private key (103, 143)
$= (97)^{103} \bmod 143$
$= (97)(97)^{51})\ (97)^{51})$
$= (97)\ ((97)\ (97)^{25}(97)^{25})^2$
$= (97)\ ((97)\ (97)^{25}(97)^{25})^2$
….
$(97)^{103} mod\ 143 = 124$

C = 124

Decryption
C = 124, Public Key = (7, 143)
$= (124)^7 \bmod 143$
$= 124((124)^3)^2 \bmod 143$

$124^3 \bmod 143 = 5$
$124^6 \bmod 143 = 25$
$(124)^7 \bmod 143 = 124*25 \bmod 143 = 97$

We got back the message M = 97