Assignment 4

Yang David Zhou, ID 260517397

November 6, 2014

Problem 1. *Primality Testing.*

Solution. (a) $a = 5$, $n = 124$ in $a^{n-1} \equiv 1 \mod n$
$5^{124-1} \mod 124$
Since 5 is clearly not divisible by 124, we can apply Fermat's Little Theorem.
$\equiv 1 \mod 124$
For $a = 5$, $n = 124$ passes the test.

(b) The test did not give the correct answer since 124 is clearly an even number and therefore not prime. This is an example of a liar number and the reason why the Fermat Primality Test is probabilistic.

Problem 2. *RSA Encryption.*

Solution. (a) Encryption is $\hat{M} = M^p \mod n$ with $\{n = 91, p = 5\}$
$\hat{M} = 4^5 \mod 91$
$= 4^4 \cdot 4 \mod 91$
$= (4^4 \mod 91 \cdot 4 \mod 91) \mod 91$
$= ((4^2 \mod 91 \cdot 4^2 \mod 91) \mod 91 \cdot 4 \mod 91) \mod 91$
$= (74 \cdot 4) \mod 91$
$= 296 \mod 91$
$\hat{M} = 23$

(b) We use the modular inverse of $p \mod (q_1 - 1)(q_2 - 2)$ so $x = 5^{-1} \mod 72$

$\gcd(72, 5)$
$= \gcd(5, 2)$
$= \gcd(2, 1)$
$= \gcd(1, 0)$
$= 1$

$1 = 5 - 2 \cdot 2$
$= 5 - 2 \cdot (72 - 14 \cdot 5)$
$1 = 29 \cdot 5 - 2 \cdot 72)$
So we use $x = 29$

(c) Decryption is $M = \hat{M}^x \mod n$ with $n = 91, x = 29$
$M = 23^{29} \mod 91$
$M = 23^{16} \cdot 23^8 \cdot 23^4 \cdot 23 \mod 91$

[Aside]
$23^2 \mod 91 = 74$
$23^4 \mod 91 = (23^2 \mod 91 \cdot 23^2 \mod 91) \mod 91 = 16$
$23^8 \mod 91 = (23^4 \mod 91 \cdot 23^4 \mod 91) \mod 91 = 74$
$23^{16} \mod 91 = (23^8 \mod 91 \cdot 23^8 \mod 91) \mod 91 = 16$

$M = 16 \cdot 74 \cdot 16 \cdot 23 \mod 91$
$M = 16 \cdot 23 \mod 91$
$M = 368 \mod 91$
$M = 4$

Problem 3. *A Combinatorial Identity.*

Solution. (a) We observe that,
$\binom{n}{0} \cdot 2^0 + \binom{n}{1} \cdot 2^1 + ... + \binom{n}{n} \cdot 2^n = 3^n$
Can be rewritten as,
$(1+2)^n = \sum_{k=0}^{n} \binom{n}{k} 2^k$
Which is simply the binomial theorem when $x = 1, y = 2$. The equality in the binomial theorem was proven in class.
(b) In the form,
$3^n = \sum_{k=0}^{n} \binom{n}{k} 2^k$
The LHS can be viewed as counting the number of possible sequences in a n-tumbler combination lock where each tumbler is either $\{0, 1, 2\}$.

The RHS also counts the possible sequences. The number of ways to choose k tumblers that is either a 0 or a 1 is $\binom{n}{k}$. In each of these choices there are a further 2^k ways to assign a 0 or a 1 to the tumblers. So the term $\binom{n}{k} 2^k$ counts both the combinations of having k 0s and 1s and the $n - k$ tumblers that have a 2 since 2 is the only choice possible for the unassigned $n - k$ tumblers. Summing up the $k = 0...n$ terms gives all the possible sequences.