CS 402 Cryptography

Problem Sheet 6

(1) What is a *pseudoprime*? A *Carmichael number*?

(2) Find all bases b for which 15 is a pseudoprime.

(3) Prove that there are 36 bases for which 91 is a pseudoprime.

(4) Show that if p and $2p-1$ are both prime, then $n = p(2p-1)$ is a pseudoprime for 50% of all possible bases.

(5) Suppose that for k choices of base b, the odd composite integer n satisfies $b^{n-1} \equiv 1 \bmod n$. If n is not a Carmichael number, show that the probability that n is prime is at least $1 - \frac{1}{2^k}$. Discuss how this fact can be used in a probabilistic primality test.

(6) Let $n = pq$ where p and q are primes, $p \neq q$. Set $d = \gcd(p-1, q-1)$. Let b be an integer coprime to n, $1 < b < n$. Prove that n is pseudoprime to the base b if and only if $b^d \equiv 1 \bmod n$.

(7) Prove that 561 is the smallest Carmichael number.

(8) Suppose m is a positive integer such that $6m+1$, $12m+1$, and $18m+1$ are all primes. Prove that $n = (6m+1)(12m+1)(18m+1)$ is a Carmichael number.

(9) Show that the following are Carmichael numbers:
(i) 1105, (ii) 1729, (iii) 2465, (iv) 2821, (v) 6601, (vi) 29341, (vii) 278545.

(10) Consider the following procedure.

Input: an odd integer $n > 1$.
Output: a factor of n that is not 1 or n; or a message that n is prime.
Method:

$x \leftarrow [\sqrt{n}\,]$

1. If $\sqrt{n}$ is an integer, then $\sqrt{n}$ is a factor of n: STOP.
2. $x \leftarrow x + 1$.
3. If $x = (n+1)/2$ then n is prime: STOP.
4. If $y := \sqrt{x^2 - n}$ is an integer then $x + y$ and $x - y$ are factors of n: STOP. Otherwise, GOTO Step 2.

Prove that this procedure terminates (what would happen if an even integer n were input?). Also show that the procedure correctly determines that n is prime if it is indeed prime, and correctly determines proper factors of n if n is composite.

(11) Use the algorithm in the previous question to find factors of
(i) 175557, (ii) 455621, (iii) 731021.