MATH 195: CRYPTOGRAPHY
HOMEWORK #7

Problem 6.22. *A* Carmichael number *is an integer* $n > 1$ *that is* not *prime with the property that for all* $a \in \mathbb{Z}$, $a^n \equiv a \pmod{n}$. *Prove that* $561, 1105, 1729$ *are Carmichael numbers. [Hint: Look at the proof of* $a^{ed} \equiv a \pmod{n}$, $n = pq$, *in the RSA-scheme. You may use the prime factorization of these numbers.]*

Problem 6.23. *Show that 'in practice' Carmichael numbers are easy to factor into primes. Illustrate the method on one of* $561, 1105, 1729$.

Problem 6.24. *Let* n *be an RSA modulus,* e_1 *an encryption exponent,* d_1 *the corresponding decryption exponent, and* e_2 *a second encryption exponent. Exhibit a fast and* certain *algorithm that determines a decryption exponent* d_2 *(*not *using random choices, or the factorization of* n*, or exponentiation modulo* n*). Illustrate your algorithm on* $n = 119$, $e_1 = 23$, $d_1 = 23$, $e_2 = 7$ *and* $n = 119$, $e_1 = 23$, $d_1 = 23$, $e_2 = 11$.

Date: March 12, 2002.

6.22, 6.23, 6.24.