18.704 Fall 2004 Homework 9

All references are to the textbook "Rational Points on Elliptic Curves" by Silverman and Tate, Springer Verlag, 1992. Problems marked **(*)** are more challenging exercises that are optional but not required.

1. A *Carmichael number* is an integer $n \geq 1$ such that $a^{n-1} \equiv 1 (\bmod n)$ holds for all a relatively prime to n. FYI: I believe the question of whether there exist infinitely many Carmichael numbers is an open problem.

(a) Suppose that $n = p_1 p_2 \dots p_r$ is a product of r *distinct* primes. Show that n is a Carmichael number if and only if $p_i - 1$ divides $n - 1$ for each i (hint: look up Fermat's Little Theorem and the Chinese Remainder Theorem if you don't know these.) Find a product of three distinct primes which is a Carmichael number (there exist several possibilities with all three primes less than 20.)

(b) Show that no product of two distinct primes is a Carmichael number.

2. Do Exercise 5.5 (a) and (b) from the text.

3. Do Exercise 5.4 from the text.