Computer Algebra
Spring 2010
Assignment Sheet 3

Exercises marked with a ★ can be handed in for bonus points. Due date is April 13.

Exercise 1
Prof. Magma claims that peasant’s multiplication and fast modular exponentiation are the same algorithm. What do you think of that, and why?

Exercise 2 (★)
Determine the remainder that one gets when dividing $2^{15 \times 313 \times 379 \times 409 \times 105}$ by 101.

Exercise 3
Let $N = pq$, where $p \neq q$ are primes. Show that given only $N$ and $\phi(N)$, one can efficiently compute the prime factors $p$ and $q$.

Exercise 4
Let $N = pq$, where $p \neq q$ are primes, and let $e \neq d$ be natural numbers such that $ed \equiv 1 \mod \phi(N)$.

1. Show that given only $N$, $e$, and $d$, one can efficiently compute the prime factorization of $N$.

2. What does this say about how hard it is to find the private key in RSA encryption? What about the hardness of breaking RSA encryption? Discuss.

Exercise 5 (★)
Show that if $p$ and $2p - 1$ are both prime and $N = p(2p - 1)$, then exactly half of the elements of $\mathbb{Z}_N^*$ are Fermat liars, namely all those which are squares modulo $2p - 1$.

Exercise 6
Let $N = p^k$ where $p$ is prime. Show that $N$ is not a Carmichael number.