Math 343L – final exam – to be written on Friday, Dec 9 2011.

1. Compute $11^{1000} \pmod{101}$.

2. We have discussed the balance between cryptographic security (which requires permuting elements of a large space of words) and computational ease (which requires that the permutation be expressed and computed with just a few operations available in a computer). In this problem we will see that there do indeed exist some "hard" permutations.

(a) Approximately how many permutations are there on the set of all 8-bit bytes? Express your answer in scientific notation. (You may find Stirling's Approximation, and a calculator, to be useful.)

(b) The set W of 8-bit bytes can be identified with Z_{256}, or with the field F of 2^8 elements. In either case, we can obtain a permutation of W by using a translation $(x \to x + c\ )$ or a scaling $(x \to a \cdot x\ )$ or a power operation $(x \to x^b)$; choosing different values of a, b, or c will give different permutations. Let P be the set of all the permutations that are of one of these three types. Give an upper bound on the number of elements in P. (It can only be an upper bound unless you can tell for sure that for example no scaling is also a power map.)

(c) The composite of permutations is again a permutation. Give an upper bound on the number of permutations that can be formed by composing two elements of P.

(d) Generalize your thinking in (c) to conclude that there are permutations of the set W that cannot be computed with fewer than 100 arithmetic operations (i.e. which cannot be written as a composite of fewer than 100 elements of set P).

3. Alice has decided to use RSA to receive secret messages. She has announced publicly that messages, viewed as sequences of integers modulo $2047 = 2^{11} - 1$, should be sent to her encrypted: to convey the message integer m, you should transmit the encrypted message $m^3 \pmod{2047}$. Sadly for Alice, she forgot that you know some number theory. Explain how you could decrypt any messages you intercept on their way to Alice — how can you compute cube roots modulo 2047? (Do not use a look-up table; of course you could do that since our m is one of only 2047 possible values, but you should demonstrate that you know how to do this with any modulus that you can factor!)

4. Find four solutions to the equation $x^2 = 9$ in Z_{91}. (Hint: $91 = 7 \cdot 13$.)

5. In class we proved that the cardinality q of a finite field F must be a power of some prime p. Show that the function

$$\phi : F \to F \qquad \text{given by} \qquad \phi(x) = x^p$$

preserves addition and multiplication, i.e. $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$. (This ϕ is called the *Frobenius automorphism* of F.) Give a concrete description of what function ϕ is when $F = Z_p$, and also when F is the field of four elements which we constructed in class.

6. Recall that the mechanism used to turn an elliptic curve into a *group* (the drawing of lines) works whenever the defining equation of the curve is a polynomial of degree 3 in x and y. In particular, the equation $x^3 + y^3 = 1$ defines an elliptic curve. Explain why the only points on this curve that have rational coordinates are $(0, 1)$ and $(1, 0)$. (You may wish to look up "Fermat's Last Theorem", which was proven for the exponent 3 by Euler, and later for all exponents by Wiles and Ribet. You may use this theorem without understanding the proof, although it is interesting to note that the proof started by Ribet and completed by Wiles is very much in the language of elliptic curves!)