THEORY OF NUMBERS, Math 115 B
Homework

1. Explain in your own words what is a public-key encryption system.
2. What is the knapsack problem?
3. (8.5.2) Show that if $a_1, a_2, \ldots, a_n$ is a super-increasing sequence, then $a_j \geq 2^{j-1}$ for $j = 1, 2, \ldots, n$.
4. (8.5.6) Encrypt the message BUY NOW using the knapsack cipher based on the sequence obtained from the super-increasing sequence $(17, 19, 37, 81, 160)$ by performing modular multiplication with multiplier $w = 29$ and modulus $m = 331$.
5. (9.1.4) Find a primitive root modulo each of the following integers: 4,5,10,13,14,18.
6. (9.1.5) Show that 20 has no primitive roots.
7. (9.1.16) Show that if r is a primitive root modulo the positive integers m, then r^{-1} is also a primitive root modulo m.
8. (9.2.1) Find the number of incongruent roots modulo 11 of each of the following polynomials $x^2 + 10$ and $x^4 + x^2 + 1$.
9. What is a discrete logarithm and why is it interesting for cryptographic applications?