HW 1: due Thursday, February 16

Problems: Submit hard copy of answers to problems 1-4. For Problems 2 and 3, please in addition use `provide` to submit the source code of your programs. This works from any EECS machine by typing:

```
sun% provide comp150cs hw1 myfilename1.here myfilename2.here ..
```

1. By hand, using the method of repeated squaring, compute 3^{29} mod 100. Show your work.

2. Write a program that takes as input an integer modulus n, a positive integer x, and an integer exponent a and computes x^a mod n by the method of repeated squaring. What does your program output when $n = 27001$, $x = 101$ and $a = 21768$?

3. Write a program with integer inputs x and n and y, outputs an answer to the question: for which positive integer values of $a < n$ does x^a mod $n = y$? (Note: I am not assuming that you can find a particularly efficient or good algorithm for this problem!) Use your program to answer: for x = 101 and n = 27001, for which values of a does x^a mod $n = 12000$? Is 101 a generator mod 27001? Compare the running time of this program with the program you wrote for the previous problem.

4. Write down the multiplication tables for $Z_{11}\backslash\{0\}$, $Z_6\backslash\{0\}$ and Z_8^*. Which of these sets form a group under multiplication, and why?