Math 156
Fall 2001

Name ____________________

Test 2

Be sure to show your work on all problems. Unsubstantiated answers will not receive full credit.

1. a) What is 148 mod 16?

b) What is -37 mod 16?

2. a) The inverse of 27 mod 100 is one of the following five numbers. Which one? Make sure your answer indicates how you know; guesses will receive no credit.

13 37 63 71 97

b) **Use your result from part (a)** to find the smallest positive integer x such that $27x \equiv 34 \pmod{100}$.

3. Find the **two smallest** positive integers z such that $z \equiv 0 \pmod{100}$, $z \equiv 4 \pmod{11}$, and $z \equiv 3 \pmod{13}$.

4. $a_0 = 5$, $a_1 = 4$, and when $n \geq 2$, $a_n = a_{n-1} + 2a_{n-2}$.

a) What are a_2 and a_3?

b) Find a closed form expression for a_n (i.e., a formula that allows us to compute a_n directly from n).

5. Compute 5^{26} mod 7 two diferent ways: a) using **repeated squaring**, and b) using **Fermat's Little Theorem**. Be sure to show your work carefully.

6. Answer the following about RSA. **Your answers should indicate the relationships between the various pieces of information.**

a) To set up an RSA system, what information do you need?

b) What information do you make public?

c) What information do you keep private?

d) How do you generate the code block C of a message block M? (Assume M is the numeric equivalent of some message – you don't have to explain how to convert an ASCII block into a number.)

e) How do you decode C?

f) What must one prove to show that RSA encryption/decryption works? (You don't have to actually give the proof.)

7. a) Give a formula that allows for easy computation of $\sum_{i=0}^{k} r^i = 1 + r + r^2 + \cdots + r^k$.

b) Use the formula to determine the *exact* value of $\sum_{i=0}^{15} (\frac{1}{3})^i = 1 + \frac{1}{3} + (\frac{1}{3})^2 + \cdots + (\frac{1}{3})^{15}$. (Do not give a decimal approximation.)

c) Show why the formula is valid. (That is, prove that the formula works.)

8. A standard deck of cards has 52 cards (4 suits of 13 kinds each). In poker, a full house is 3 of one kind of card and 2 of another kind (e.g. 5 of hears, 5 of diamonds, 5 of clubs, 8 of spades, 8 of hearts). How many different full houses are there?

9. $g(1) = 2$ and $g(n) = 3g(n/3) + n$ when n is divisible by 3.

a) What is $g(27)$?

b) Use unraveling to find an *exact* formula for $g(n)$ (when n is a power of 3) If you cannot do this, then for partial credit you may give a good Big O estimate.