The problems below are problems I have used in the past on quizzes and tests in Math 156 and represent some of the kinds of things that could occur on Test 2.

1. Write three mathematical statements that are equivalent to $a \equiv b \pmod{n}$.

2. Use Euclid's algorithm to find the gcd of 286 and 234.

3. a) Show that 9 is the inverse of 11 mod 14.

b) Use this to solve $11x \equiv 3 \pmod{14}$.

4. 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 to a number.)

e) How do you decode C?

5. a) Show that 29 is the inverse of 11 mod 53.

b) Use the fact that 29 is the inverse of 11 to find a number x between 0 and 53 such that $29x \equiv 9 \pmod{53}$.

6. Show how to use repeated squaring to compute $5^{10} \pmod{15}$.

7. Use the information below to find a number x such that $0 \leq x < 55$ and $23x \equiv 7 \pmod{55}$.

```
55 = 2 * 23 + 9
                          9 =  1 * 55  -  2 * 23
23 = 2 * 9 + 5
                          5 = -2 * 55  +  5 * 23
 9 = 1 * 5 + 4
                          4 =  3 * 55  -  7 * 23
 5 = 1 * 4 + 1
                          1 = -5 * 55  + 12 * 23
 4 = 4 * 1 + 0
                          0 = 23 * 55  - 55 * 23
```

8. Show that if $a \equiv x \pmod{m}$ and $b \equiv y \pmod{m}$, then $ab \equiv xy \pmod{m}$.

9. Use induction to show that for any $n \geq 1$,

$$\sum_{i=1}^{n} \frac{1}{i^2} = 1 + \frac{1}{4} + \frac{1}{9} + \cdots \frac{1}{n^2} \leq 2 - \frac{1}{n}$$

[Notice that this implies that $\sum_{i=1}^{\infty} \frac{1}{i^2} \leq 2$.]

10. Use induction to show that the sum of the first n even numbers is $n^2 + n$. That is, for any $n \geq 0$,

$$\sum_{i=0}^{n} 2i = 0 + 2 + 4 + \cdots 2n = n^2 + n \ .$$

11. a) How many license plate "numbers" are possible if the numbers consists of three letters followed by 3 digits? (Example: ABC 123)

b) How many of these repeat either a letter or a digit? (Examples: KKM 475 or ABC 151 or ZZZ 123, etc. Repeated numbers or letters do not need to be consecutive and may appear either two or three times.)

12. a) Two of the following four numbers are inverses of each other mod 1000. Which two?

371 469 531 625

b) One of the numbers above has no inverse mod 1000. Which one and why?

c) Why are inverses important? Give an example of a situation where knowing the inverses in part a) could be useful. That is, make an example problem and solve it.

13. Consider the following recurrence.

$$a_0 = 3; a_1 = 8; a_n = 6a_{n-1} - 8a_{n-2} \quad (n \geq 2)$$

a) What are a_2 and a_3?

b) Find a closed form expression for a_n.

14. Which of the following are linear homogeneous recurrence relations? For the ones that are, give their degree. For the ones that are not, explain why not.

a) $a_0 = 0;\ \ a_1 = 1;\ \ a_n = 3a_{n-1} + 4a_{n-2} \ \ (n \geq 2)$

b) $b_0 = 0;\ \ b_1 = 1;\ \ b_n = 4b_{n-1}b_{n-2} \ \ (n \geq 2)$

c) $c_n = 1 \ \ (0 \leq n \leq 4);\ \ c_n = 4c_{n-3} - 2c_{n-5} \ \ (n \geq 5)$

d) $d_0 = 0;\ \ d_1 = 1;\ \ d_n = 2d_{n-1} + 3d_{n-2} + 4 \ \ (n \geq 2)$