Student ID Number
-------------------

Name:\_\_\_\_

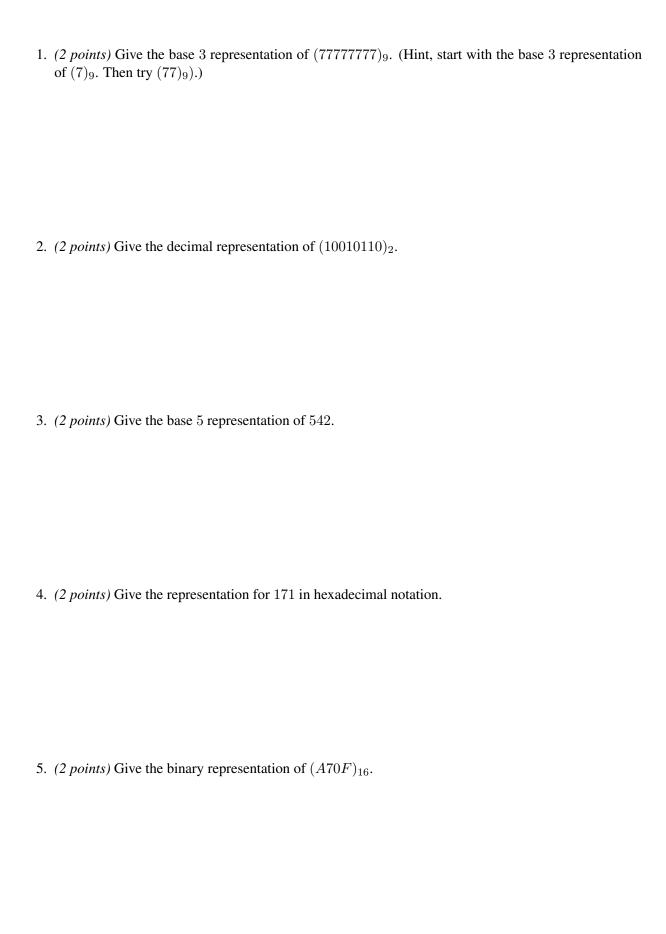
## Test II

ICS 6D Spring 2015 Wed, May 13, 2015

Instructor: Sandy Irani

Wait until instructed to turn over the cover page. Complete all of the following questions. There are a total of 50 points.

Page 1	
Page 2	
Page 3	
Page 4	
Total	



6. (2 points) Circle the numbers below that are equivalent to 3 mod 11:

58

-7

11

113

-3

-11

-30

7. (8 points) Compute the following quantities:

(a)  $-127 \mod 11$ .

(b) -127 div 11.

(c)  $(25 - 1700 * 265^2) \mod 17$ .

(d)  $(56 - 3 * 34) \mod 11$ .

8. (5 points) Compute  $(46)^{39} \mod 11$ 

9. (3 points) Compute  $7^{36} \mod 2399$ . The following equalities may be useful:

$$7^2 \mod 2399 = 49$$
  $7^{16} \mod 2399 = 16$   $7^4 \mod 2399 = 2$   $7^{32} \mod 2399 = 256$   $7^8 \mod 2399 = 4$   $7^{64} \mod 2399 = 512$ 

10. (6 points) Use the prime factorizations given below to compute the following expressions:

$$19800 = 2^{3} \cdot 3 \cdot 11 \cdot 15^{2}$$

$$4590 = 2 \cdot 3^{2} \cdot 11^{2} \cdot 17$$

$$3267 = 3^{3} \cdot 11^{2}$$

- (a) Give the prime factorization for lcm(19800, 3267).
- (b) Give the prime factorization for gcd(19800, 4590).
- (c) Give the prime factorization for  $4590 \cdot 3267$ .
- 11. (4 points) Consider an RSA cryptostystem with public key (e, N), where  $N = p \cdot q$  and p and q are prime. The private key is d. Alice wishes to send a plaintext message m to Bob.
  - (a) Give an expression for the cyphertext message that Alice sends as a function of the parameters above.
  - (b) If Bob receives cyphertext c, give an expression for m, the original plaintext message, as a function of c and the other parameters besides m.

12. (12 points) Consider an RSA cryptosystem with p=11 and q=13. Suppose that the encryption key e=83. Compute the decryption key d. Your answer should be a non-negative number.

Show all your work as clearly as possible, so you can get partial credit if needed.