family name ______________ given name ______________ ID ______________

cmput204 2014oct17 45min no electronics SHOW ALL WORK

1. Multiply the binary number below by two. Give your answer in binary.

```
   x =     1  1 1 0 1  0 1 1 0  0 1 1 1
10*x =
```

2. As a function of k, using $\Theta(\,)$ notation, how long would it take you to multiply a k-bit binary number by two?

____

```
def q(x,y): # x >= 1
  if x==1: return y
  z = 2*q(x/2,y)
  if (1==x%2): z = z+y
  print x,y,z
  return z
```

3. Show the output from `q(13,8)`.

Rough work: Final answer:

4. Give (but do **not** solve) a recurrence relation for the runtime $T(n)$ of `q(n,y)`. Assume that all operations inside the body take time proportional to the number of bits of the numbers being operated on. Use $\Theta()$ or $O()$ notation.

```
T(n) =                                         if n=1

     =                                         if n >= 2
```

5. Compute $37^{198} \pmod{41}$. Hint: $37^{99} \pmod{41} = 10$.

6. For how many numbers x in $\{2, 3, \ldots, 8\}$ does $x^9 = 1 \pmod{10}$?

7. For how many numbers x in $\{2, 3, \ldots, 39\}$ does $x^{40} = 1 \pmod{41}$? Explain.

8.

```
def isp(b,t):
  found, tries = False, 0
  while not found:
    n = random.randint(2**(b-1)+1, 2**b-1)
    if (0==n%2): n=n+1  # ???
    found, tries = True, tries+1
    for _ in range(t):
      a = random.randint(2,n-2)
      if (1!= pow(a,n-1,n)): found = False
  return n, tries
```

(i) Explain the purpose of the line marked `???`.

(ii) Give a rough bound on the probability that the `n` returned by `isp(33,10)` is prime.

(iii) Estimate the average value of `tries` returned by `isp(33,10)`. Explain briefly.

9. A divide and conquer algorithm takes an input of size $n = 3^t$. If n is at most 27, it returns the answer in constant time. For larger n, it recursively solves 9 subproblems each with size $n/3$, and then takes $\Theta(n^2)$ time to transform those solutions into the final solution.

   (i) Give a recurrence relation for the runtime.

   (ii) Using $\Theta(\,)$ notation, as a function of n, give the runtime.

10. (i) Let a, b, x, y be integers such that $ax + by = 1$. Let d be a positive integer that divides both x and y. Prove that $d = 1$.

    (ii) Let `x=35267`. Let `y=21119`. Notice that `x * 2563 = 90389321`, and `y * 4280 = 90389320`. Find an integer `z` such that `y*z = 1 (mod x)`, or explain why no such integer exists.

11. For each $f(n)$, give the simplest $g(n)$ so that $f(n) = \Theta(g(n))$.

    (i) $16\,n^2 \lg n \;+\; 11\,n^2$ $g(n) =$

    (ii) $n^2 \lg n \;+\; 5^{\lg n}$ $g(n) =$

    (iii) $9 \displaystyle\sum_{j=1}^{n} j^4 \lg j$ $g(n) =$