CS 310
Homework Assignment No. 3
Due on Tue 2/4/2003

1. Write a *recursive* algorithm that computes the greatest common divisor of two non-negative integers, not both zero, that uses subtractions but not modulus operations.

2. Give a Θ notation of the form $\Theta(n^k)$ ($k \in \mathbb{Z}$) for the number of times the statement '`x := x+1`' is executed in the following algorithm:

```
1: procedure silly_loop(n)
2:   x := 0
3:   for i:=1 to n do
4:     for j:=1 to 10*i*i do
5:       for k:=1 to 2*j do
6:         x := x+1
7: end silly_loop
```

3. Prove that the number of times the basic steps **return**`(0)` and **return**`(1)` will be executed during the execution of the following algorithm is $\Omega(2^{n/2})$ and $O(2^n)$.

```
1: procedure fibonacci(n)
2:   if n=0 then
3:     return(0)
4:   if n=1 then
5:     return(1)
6:   return(fibonacci(n-1) + fibonacci(n-2))
7: end fibonacci
```

4. You need to pour exactly 1 floz of water into a pot, but you only have two containers with capacity for 36 floz and 49 floz respectively. You are allowed to transfer water among the containers as you wish, but you cannot measure directly any amount of water that is a fraction of one of the containers. Pose the problem as a Diophantine equation, solve it, and use the solution to find a way of measuring exactly 1 floz with the two containers.

5. We have a number of stamps of various denominations and want to mail a package that requires \$3.25 postage. In each of the following cases determine if we have the appropriate stamps to get exactly the required postage. Justify the answers.
(a) 1000 8¢-stamps, 500 10¢-stamps and 300 22¢-stamps.
(b) 20 15¢-stamps and 5 50¢-stamps.
(c) 100 50¢-stamps and 100 33¢-stamps.
(d) 4 50¢-stamps and 4 35¢-stamps.

(next page →)

6. We have intercepted a secret message from the enemy encrypted with the RSA algorithm. The encoding is $A = 01, B = 02, C = 03, \ldots, Z = 26$, and the public encryption key used by the enemy is $(n, e) = (31732031, 29553281)$. For instance, the word DOG would be encrypted as follows. First it is encoded: $DOG = 041507$. Then it is encrypted: $041507^{29553281} \bmod 31732031 = 5470487$. The encrypted message that we have intercepted is $m' = m^e \bmod 31732031 = 18091168$. Your mission is to decrypt (and decode) the message. In order to do that, use the following steps (you will need some computer algebra system such as Maple to do the computations):[1]

(1) Find the prime factors p and q of $n = 31732031$.
(2) Find $\phi(n)$.
(3) Find $d = e^{-1} \bmod \phi(n)$. The decryption key is (n, d).
(4) Decrypt the secret message by computing $m = {m'}^d \bmod n$.[2]

[1] In Maple you may use "`ifactor`" to find the prime factors of n, and "`mod`" for computations modulo n. Remember to use the ampersand in expressions of the form "`a&^b mod n`" in Maple (so that Maple uses the efficient algorithm to compute powers modulo n.) Basically, the computations to be performed are: find p and q with "`ifactor(n)`", find $\phi(n) =$ "`(p-1)*(q-1)`", find $d =$ "`e&^(-1) mod` $\phi(n)$", find $m =$ "`m'&^d mod` n". Finally, decode m.

[2] Note that you managed to decode the message because you were able to factor n—so if you want to develop a secure implementation of the RSA algorithm you must choose an n that is hard to factor; in particular the prime numbers p and q should be very large.