

## Practice Problem Set 1

Date - January 13, 2013

1. Write a function (has\_solution a b c) which returns #t if the diophantine eqn.  $ax + by = c$  has solutions for integer values of  $x$  and  $y$ .

HINT: The diophantine equation  $ax+by=c$  has a solution for integer values of  $x$  and  $y$ , if  $\text{gcd}(a,b)$  divides  $c$ .

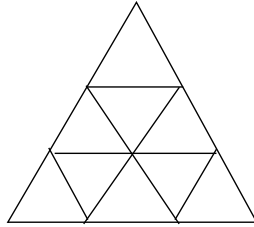
2. Write a function (sub x y) which subtracts  $y$  from  $x$ . You can assume that  $x$  is larger than  $y$ . Define sub in terms of an appropriate function (sub-single x y z) with constraints on the values of  $x$ ,  $y$ , and  $z$ . The function should check these constraints. You can also use the function convert to left-shift and add.
3. Write a function (ak-mult x y) to multiply two numbers using the Al-Khwarizmi method.
4. Define a function (div x y),  $y$  is not 0, which will return a pair of numbers  $(q,r)$  such that  $x = yq + r$  and  $r < y$ . This should also work by repeated halvings of  $x$ .

- 
5. Given two numbers  $a$  and  $b$ , write a function coeffs which will return a pair of numbers  $x$  and  $y$  such that  $a*x + b*y = \text{gcd}(a,b)$
  6. Given two integers  $x$  and  $n$  and an integer exponent  $y$ , write a function (modexp x y n) which will output:  $x^y \bmod n$ .
  7. A Carmichael number is a non-prime number  $p$  such that for every  $1 \leq a \leq p$ ,  $a^{p-1} = 1 \bmod p$ . Define a function (carmichael n) which will give the  $n$ th Carmichael number.
  8. Write a function (inverse e n) which will return the inverse of  $e$  modulo  $n$ .
  9. Write a function (is-prime n) to implement the Fermat's little theorem based probabilistic algorithm to test whether  $n$  is a prime. Assume that  $n$  is not a Carmichael number. Use the function (random k) to generate a random number in the range  $0..k-1$ .
  10. Suppose that the RSA algorithm uses the prime numbers  $p$  and  $q$  to generate the encryption, the encoding exponent is  $e$  and the code of a message (a number) is  $c$ . Write a function (decode p q e c) to decode the message.

11. Goldbach's conjecture says that every positive even number greater than 2 is the sum of two prime numbers. Example:  $28 = 5 + 23$ . It is one of the most famous facts in number theory that has not been proved to be correct in the general case. It has been numerically confirmed up to very large numbers (much larger than we can go with our Scheme system). Write a function (goldbach m) to find the two prime numbers that sum up to a given number m. Use the magic function cons to pack a pair of numbers.
12. Write a function (minchange n) which will return the minimum number of coins required to give change of n paise. You are given sufficient numbers of 1p, 2p, 3p, 5p, 10p, 20p, 25p, and 50p coins. For how high a value of n can you go in 5 minutes of computation time?
13. The Josephus problem is described as follows: n people numbered 1 to n are made to stand in a circle. Starting from the person numbered 1, every third live person is killed. This is done till only two persons are left. As an example, if n is 15, then the survivors are the persons who were originally at positions 5 and 14. Your job is to write a function (cansurvive pos n) that takes as its arguments a position pos and the number of people n, and returns #t if the person at position pos is one of the last two survivors; otherwise it returns #f.
14. Euler's totient function. Euler's so-called totient function  $\phi(m)$  is defined as the number of positive integers r ( $1 \leq r < m$ ) that are coprime to m.
- Example:  $m = 10$ :  $r = 1, 3, 7, 9$ ; thus  $\phi(m) = 4$ . Note the special case:  $\phi(1) = 1$ .
15. Assume that we represent a rational number  $p/q$  as (cons p q). With this representation, define the following functions on rational numbers.
- (simplify r) - converts a rational number r into its simplest form.  $12/18$  simplifies to  $2/3$ .
  - (add r1 r2) - adds two rational numbers r1 and r2.
  - (multiply r1 r2) - multiplies two rational numbers.
  - (divide r1 r2) - divides r1 by r2.

- 
16. Consider the diagram shown below. Assume all triangles in the diagram are equilateral. The outermost triangle is of height 3. It contains 9 triangles of height 1, of which 3 are inverted. It also contains 3 triangles of height 2 of which none are inverted. Thus a triangle of height 3 contains  $9+3+1=13$  triangles including itself. If (triangles h) is a function which gives the total

number of triangles contained in a triangle of height  $h$ , then  
(triangles 3) = 13. Similarly, you can verify for yourself that  
(triangles 4) = 27.



- a. What is (triangles 5)?
- b. Define triangles. Try to define it in such a way that triangles gives an answer for large values(e.g. 10000000) in a reasonable amount of time, say a minute.