Problem Set 5  (Solutions are due Wed. 3-05-08)

1) Exponentiation $y = x^e$ in $\mathbb{Z}_n$. The following Matlab function implements a fast algorithm to compute $x^e \pmod{n}$ for $e \geq 0$ and $n \geq 2$.

```matlab
function y = x2en(x,e,n)
% x2en Computes y=x.^e (mod n) for e>=0 and n>=2.

y = ones(size(x));
z = x;
while e>0
    if mod(e,2)==1
        y = mod(z.*y,n);
    end
    z = mod(z.*z,n);
e = floor(e/2);
end
```

(a) Explain how the algorithm works.
(b) Compute $y$ for $x = 84754$, $e = 40698$, $n = 98207$.
(c) How many multiplications does the algorithm have to perform at most? How does that compare to the number needed for the brute force computation $x^e = x \cdot x \cdot x \cdots x$?

2) Using the Chinese remainder theorem, develop an algorithm to find $\sqrt{a}$ modulo $n$, $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, assuming that $a \in QR_n$ and assuming that it is possible to find $\sqrt{a}$ modulo $p_i^{e_i}$, $i = 1, 2, \ldots, k$, easily. Apply this to find $\sqrt{217611390}$ modulo $595973171$.

3) Problem 5.4 in the book by Wenbo Mao. Let $n$ be a odd composite integer which is not a power of a prime (i.e., $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with $k \geq 2$). Does the group $\mathbb{Z}_n^*$ have a generator? (A different formulation of the same question would be: Is the group $\mathbb{Z}_n^*$ cyclic?)