Carolyn Tang/ct180
Jason Wang/jsw50
Problem Set 2

Written Exercise

```
(define exptmod
   (lambda ((b <integer>) (e <integer>) (m <integer>))
     (cond ((zero? e) 1)
           ((even? e)
            (modulo (square (exptmod b (quotient e 2) m)) m))
           (else
            (modulo (* b (exptmod b (- e 1) m)) m)))))
```

<u>Base Case:</u>
Prove that (exptmod b {0} m) = modulo(b^0, m) = modulo(1, m) = 1
(exptmod b {0} m) by the substitution model is:
(cond ((zero? e) 1) …) so (exptmod b {0} m) = {1}
So therefore that is right as 1 = 1

<u>Inductive Hypothesis:</u>
There exists k, an element of the set of all natural numbers such that
(exptmod b k m) = modulo(b^k, m)

<u>Inductive Step:</u>

Prove (exptmod b (+ k 1) m) = modulo(b^{k+1}, m)

By the substitution model:
{PROC (b<integer> k<integer> m<integer>) exptmod b {+ k 1} m}
As k+1 > k and k is a natural number, k+1 has to be greater than 0 so:
(cond (({#f})
        ((even? …))
        (else …)

IF EVEN:

= (modulo (square (exptmod b (quotient {+ e 1} 2) m)) m))

--> (exptmod b (quotient {+ e 1} 2) m) = (modulo ($b^{(k+1)/2}$, m)) by IH so

= (modulo (square (modulo ($b^{(k+1)/2}$, m))), m)

*--> we know that: modulo(q * modulo(p, m), m) = modulo(p * q, m) so using this with:*

$q = b^{(k+1)/2}$
$p = modulo(b^{(k+1)/2}, m)$
$m = m$
We get:
= (modulo (* $b^{(k+1)/2}$ modulo($b^{(k+1)/2}$, m)), m)

*--> we know that modulo(q * modulo(p, m), m) = modulo(p * q, m), so using this again with:*
$q = b^{(k+1)/2}$
$p = b^{(k+1)/2}$
$m = m$
We get:
= (modulo ({* $b^{(k+1)/2}$ $b^{(k+1)/2}$}, m))
= (modulo b^{k+1}, m)

IF ODD:

= (modulo (* b (exptmod b (- {+ k 1} 1) m)), m))
= (modulo (* b (exptmod b k m), m)
And by the IH:
= (modulo (* b (modulo(b^k, m)), m)

*--> we know that modulo(q * modulo(p, m), m) = modulo(p * q, m), so using this again with:*
$q = b$
$p = b^k$
$m = m$
We get:
= (modulo ({* b b^k}, m)
= (modulo (b^{k+1}, m)

Therefore by induction, (exptmod b e m) = modulo(b^e, m)