Elise Brown
Gilbert Brooks III

Problem Set 2

9/20/2017

```
(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)))))
```

Use mathematical induction & substitution model to prove that

(exptmod b e m) = modulo(b^e, m)

1. What variable is being inducted on?

   e

2. What is P(e)?

   (exptmod b e m) = modulo(b^e, m) for $m > 1$

3. Prove Base Case

   ((zero? e) 1) $\rightarrow b^e = b^{\boxed{0}} = 1$ ✓

4. Induction Step

   IH: Assume that (exptmod b e m) = modulo(b^e, m) holds true for any positive number $K \leq e$

   ((even? e)

   (modulo (square (exptmod (b (quotient e 2) m)) m))

By the I.H., (exptmod b $\frac{e}{2}$ m) = modulo ($b^{e/2}$, m) because $\frac{e}{2} \leq e$.

(modulo (square (exptmod b $\boxed{\frac{e}{2}}$ m)) m)

(modulo (square modulo($b^{e/2}$, m))) m)

(modulo modulo($b^{e/2}$, m$)^2$ m))

If it can be proven that modulo(modulo (b^x, m$)^y$, m) = modulo(b^{xy}, m), then we can prove that modulo ($b^{e/2}$, m$)^2$ = modulo ($b^{\frac{e}{2}2}$, m).

Since modulo(q* modulo(p,m), m) = modulo (p*q, m), it is proven that modulo(modulo(b^x, m$)^y$, m) = modulo(b^{xy}, m).

That being said,

(modulo (modulo ($b^{\frac{e}{2}*2}$, m), m)

(modulo (modulo (b^e, m), m)

modulo (b^e, m) ✓

Go through the induction process for the else case.

(else

(modulo (* b (exptmod b $\boxed{\text{(- e 1)}}$ m)) m))

(modulo (* b $\boxed{\text{(exptmod b e-1 m)}}$) m)

By IH, (exptmod b e-1 m) = modulo(b^{e-1}, m) because $e-1 \leq e$. So,

(modulo (* b modulo (b^{e-1}, m)) m)

Since modulo (q* modulo (p, m), m) = modulo (p*q, m),

(modulo $\boxed{\text{(* b modulo(}b^{e-1}\text{, m))}}$ m)

(modulo ($\boxed{\text{(* b } b^{e-1}\text{)}}$ m))

(modulo ($\boxed{b^{e-1+1}}$ m))

modulo (b^e, m) ✓

We just proved that (exptmod b e m) = modulo(b^e, m) via strong induction. Given this proof, we know that P(e) holds true for e+1 as well.