Let's consider the function `modpow_one(a, b, c)` which computes \((a^b) \mod c\). This function has many practical applications, including being a key part of the RSA cryptography algorithm.

```c
int modpow_one(int a, int b, int c)
{
    int res = 1 % c;
    while (b > 0)
    {
        res *= a;
        res = res % c;
        b--;
    }
    return res;
}
```

Prove that this function satisfies its postcondition.
modpow_two

Now we'll look at a different implementation, modpow_two.

```c
1 int modpow_two(int a, int b, int c)
2 //@requires a >= 0 && b >= 0 && c > 0;
3 //@requires (c - 1) <= int_max()/max(a, c - 1);
4 //@ensures \result == modpow_one(a, b, c);
5 {
6     int res = 1 % c;
7     int pow = 0;
8     while (pow < b)
9           {
10             if (0 < pow && pow <= b/2) {
11                 res *= res;
12                 res = res % c;
13                 pow *= 2;
14             }
15             else {
16                 res *= a;
17                 res = res % c;
18                 pow++;
19             }
20         }
21     return res;
22 }
```

Is this function asymptotically faster than, slower than, or the same speed as modpow_one? Explain.

Write loop invariants for modpow_two.

Now, prove that if the preconditions to modpow_two are satisfied, it satisfies its postcondition.

If it helps, you can assume that \(0^0 = 0\), even though it’s actually indeterminate. You can also assume that modpow_one obeys the properties that
\[
\text{modpow_one}(a, b, c) \times a \equiv \text{modpow_one}(a, b + 1, c)
\]
\[
\text{modpow_one}(a, b, c) \times \text{modpow_one}(a, b, c) \equiv \text{modpow_one}(a, 2b, c)
\]

Questions?

If you have any more questions and we’re not out of time, ask them now. There will also be a review session on Sunday at 5pm in Rashid Auditorium (GHC 4401) if you have more questions or you want a review of some specific topic.

Exam details

The midterm is on Tuesday, during the normal lecture time (9:00-10:20). Make sure to bring a photo ID with you to the exam. Follow the list below to determine where to go on the morning of the exam.

– Recitations A-E: GHC (Gates-Hillman Center) 4401 (Rashid), the usual lecture room
– Recitation F (All of it), G (Last name A-Q): NSH (Newell-Simon Hall) 3305
– Recitation G (Last name R-Z), H (All of it): NSH (Newell-Simon Hall) 1507