> Math 418 : MAPLE Solution of Assignment #2 -- *Your NAME*

```
> restart;
```

Note: The "restart" command is not necessary, but it is useful for restarting your program if you made multiple mistakes in your computations.

Problem 5(a): Using MAPLE's power mod:

```
> Power(1234, 123456789) mod 7777;
```

$$5132 \tag{1}$$

Thus, 1234^123456789 = 5132 (mod 7777).

If we try to compute this naively, then we get an overflow error (number too large):

```
> 1234^123456789  mod 7777;
Error, cannot reallocate memory (old_size=8 new_size=162037064)
> modp(1234^123456789, 7777);
Error, cannot reallocate memory (old_size=8 new_size=162037064)
```

Problem 5(b): The following program computes a^n mod m by implementing the power mod algorithm given in class:

```
> powermod := proc(a, n, m) local ni, ai, b, i;
    ni := n; b := 1; ai := modp(a, m);
    while ni ≠ 0 do;
      if irem(ni, 2) = 1 then b := modp(b·ai, m); fi;
      ni := iquo(ni, 2); ai := modp(ai·ai, m);
   od;
    return(b); end;
```

```
powermod := proc(a, n, m)
    local ni, ai, b, i;
    ni := n;
    b := 1;
    ai := modp(a, m);
    while ni <> 0 do
        if irem(ni, 2) = 1 then b := modp(b * ai, m) end if; ni := iquo(ni, 2); ai := modp(ai
        * ai, m)
    end do;
    return b
end proc
```

(2)

Testing this for a = 7, n = 1000000 and m = 1951 yields:

```
> p1 := powermod(7, 1000000, 1951);
```

$$p1 := 797 \tag{3}$$

Thus, 7^1000000 = 797 (mod 1951)

By inspection we see that this is the same answer as obtained by the built-in command

```
> p2 := Power(7, 1000000) mod 1951;
```

$$p2 := 797 \tag{4}$$

A better way to check this is by using MAPLE's evalb command:

```
> evalb(p1 = p2);
```

$$true \tag{5}$$

Note that this also gives the correct answer for the example of part (a):

```
> powermod(1234, 123456789, 7777);
```

5132 **(6)**

```
>
>
```