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:

```maple
> Power(1234, 123456789) mod 7777;
5132
```

Thus, $1234^{123456789} \equiv 5132 \pmod{7777}$.

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

```maple
> 1234^123456789 mod 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:

```maple
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 \cdot ai, m); fi;
        ni := iquo(ni, 2); ai := modp(ai \cdot 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 \cdot ai, m) end if;
        ni := iquo(ni, 2); ai := modp(ai * ai, m);
    od;
    return b
end proc
```

Testing this for $a = 7$, $n = 10000000$ and $m = 1951$ yields:

```maple
> pl := powermod(7, 10000000, 1951);
pl := 797
```

Thus, $7^{10000000} \equiv 797 \pmod{1951}$.

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

```maple
> p2 := Power(7, 10000000) mod 1951;
p2 := 797
```

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

```maple
> evalb(pl = p2);
true
```
Note that this also gives the correct answer for the example of part (a):

\[
\text{powermod}(1234, 123456789, 7777); \quad 5132
\]