> Math 418 : MAPLE Solution of Assignment #8 -- *Your NAME*

Problem 5: Strong pseudoprimes

(a) Finding the exponent of 2 in m:

Output: the largest integer e such that 2^e|m

```
> exp2 := proc(m) local e, n;
    e := 0; n := m;
    while modp(n, 2) = 0 do;
      e := e + 1; n := n/2; od;
    return(e); end;
```

```
exp2 := proc(m)
    local e, n;
    e := 0; n := m; while modp(n, 2) = 0 do e := e + 1; n := 1/2*n end do; return e
end proc
```

(1)

Test the above program for m = 1728, m=12345, m = 12

```
> 1024·12347;
```

$$12643328 \quad \textbf{(2)}$$

```
> exp2(1728), exp2(12345), exp2(12643328);
```

$$6, 0, 10 \quad \textbf{(3)}$$

Thus, the highest power of 2 dividing 1728 is 2^6, etc.

(b) A program to test whether a given n is a strong pseudoprime to the base b.

Output: true, if n is a strong pseudoprime to the base b, and false otherwise.

```
> spsp := proc(n, b) local a, r, bs, res, s;
    a := exp2(n − 1); res := false;
    if igcd(b, n) = 1
      then if a > 0 then s := (n − 1)/2^a;
      bs := Power(b, s) mod n;
      if bs = 1 then res := true;
        else for r from 0 to a − 1 while (not res) do;
          if bs = n − 1 then res := true;
            else bs := modp(bs^2, n); fi; od; fi; fi; fi;
    return(res); end:
>
```

(c) Test the above program:

```
> n1 := 1729 : n2 := 179425261 : n3 := 2^48·1234567 + 1;
```

$$n3 := 347499717572744445953 \quad \textbf{(4)}$$

```
> b1 := 10 : b2 := 20 :
> spsp(n1, b1), spsp(n1, b2);
```

$$true, false \quad \textbf{(5)}$$

Thus, n1 = 1729 is not strong pseudoprime to the base 20, and so n2 cannot be prime.

```
> spsp(n2, b1), spsp(n2, b2);
```

$$true, true \quad \textbf{(6)}$$

Thus, n2 = 179425261 is a strong pseudoprime to the bases 10 and 20, so n2 might be prime.

```
> spsp(n3, b1), spsp(n3, b2);
```

false, false **(7)**

Thus, n3 cannot be prime.

```
> isprime(n1), isprime(n2), isprime(n3);
```

false, true, false **(8)**

Thus, n2 is a prime whereas n1 nad n2 are not.

```
>
```