> Math 418 : MAPLE Solution of Assignment #7 -- *Your NAME*

Problem 5(a): Test for pseudoprimes

The following program pseudo(n,b) checks whether n is a pseudoprime to the base b.
It returns true or false.

> $pseudo := (n, b) \rightarrow evalb(Power(b, n-1) \textbf{ mod } n = 1);$

Testing this with $n := 30857$, $b = 3$, b = 5 and b = 9:

> $pseudo(30857, 3), pseudo(30857, 5), pseudo(30857, 9);$

$$true, false, true \tag{1}$$

Thus, since n = 30857 is not a pseudoprime to the base 5, we see that n is composite.

(b) Test for Euler pseudoprimes

The following program Epseudo(n,b) checks whether n is an Euler pseudoprime to the base b.
It returns true or false.

> $with(numtheory):$

> $Epseudo := (n, b) \rightarrow evalb\left(Power\left(b, \frac{(n-1)}{2}\right) \textbf{ mod } n = modp(jacobi(b, n), n)\right);$

$$Epseudo := (n, b) \rightarrow evalb\left(Power\left(b, \frac{1}{2}\, n - \frac{1}{2}\right) \textbf{ mod } n = modp(numtheory\text{:-}jacobi(b, n), n)\right) \tag{2}$$

> $Epseudo(30857, 3), Epseudo(30857, 5), Epseudo(30857, 9);$

$$false, false, true \tag{3}$$

(c) The Solovay-Strassen primality test

```
> SolS := proc(n, k) local i, r, r1, t;
    r := rand(1 ..n); t := true;
    for i to k while t do;
      r1 := r( );
      t := Epseudo(n, r1); od;
   return(t); end:
```

> $n1 := 13999457;$
$SolS(n1, 5), SolS(n1, 10), SolS(n1, 100);$

$$n1 := 13999457$$

$$false, false, false \tag{4}$$

Thus, n1 = 13999457 is composite, as already the first test told us. In fact,
n1 = 13999457 = 113*229*541.

> $ifactor(n1);$

$$(113)\,(229)\,(541) \tag{5}$$

> $n2 := 104729;$
$SolS(n2, 5), SolS(n2, 10), SolS(n2, 100);$

$$n2 := 104729$$

$$true, true, true \tag{6}$$

Thus, we strongly suspect that n2 is prime. This is confirmed by Maple:

> $isprime(n2);$

$$true \tag{7}$$

> $n3 := 340561;$

```
SolS(n3, 5), SolS(n3, 10), SolS(n3, 100);
```

Thus, already the first test tells us that n3 is composite. In fact, n3 = 13*17*23*67 is a Carmichael number because it is squarefree and satisfies (p-1)|(n_3-1) for all p|n:

```
> ifactor(n3);
```

$$(13)\ (17)\ (23)\ (67) \tag{8}$$

```
> modp(n3 - 1, 13 - 1), modp(n3 - 1, 17 - 1), modp(n3 - 1, 23 - 1), modp(n3 - 1, 67 - 1);
```

$$0, 0, 0, 0 \tag{9}$$

```
>
```