# > Math 418 : MAPLE Solution of Assignment #5 -- *Your NAME*

**Problem 5(a):** Primitive root algorithm:
- uses MAPLE's order function in the numtheory package

```
> restart; with(numtheory) :
```

myprimroot: finds the smallest primitive root mod p.

```
> myprimroot := proc(p) local a;
    for a to p - 1 while order(a, p) <> p - 1 do; od;
    return(a); end;
```

```
myprimroot := proc(p)
    local a;
    for a to p - 1 while numtheory:-order(a, p) <> p - 1 do end do; return a
end proc
```

(1)

Test this for p1 = 48947, p2 = 48673 etc. and compare the result to MAPLE's primroot function:

```
> p1 := 48947 : p2 := 48673 : p3 := 104773 : p4 := 104831 :
> myprimroot(p1), primroot(p1);
```

2, 2 (2)

```
> myprimroot(p2), primroot(p2);
```

15, 15 (3)

```
> myprimroot(p3), primroot(p3);
```

2, 2 (4)

```
> myprimroot(p4), primroot(p4);
```

22, 22 (5)

Thus, both programs give that 2 is the smallest primitive root mod p1 and mod p3,
and that 15 is the smallest mod p2 ans that 22 is the smallest mod p4.

**Note:** Even for primes of this size, the smallest primitive root is extremely small.
For example, for the primes p in the range 104728 < p < 105098,
the sequence of the smallest primitive roots mod p never exceeds 22:

```
> seq(primroot(ithprime(k)), k = 10000 ..10030);
```

12, 3, 7, 7, 2, 3, 2, 13, 3, 3, 22, 3, 13, 2, 11, 2, 6, 2, 2, 5, 5, 3, 2, 2, 11, 2, 5, 3, 5, 7, 7 (6)

**Problem 5(b):** Find all primitve roots mod p using the *myprimroot* function

```
> allprimroots := proc(p) local ls, k, r;
    r := myprimroot(p); ls := [r];
    for k from 2 to p - 1 do;
      if igcd(k, p - 1) = 1
        then ls := [op(ls), Power(r, k) mod p]; fi; od;
    return(ls); end;
```

```
allprimroots := proc(p)
    local ls, k, r;
    r := myprimroot(p);
    ls := [r];
    for k from 2 to p - 1 do
        if igcd(k, p - 1) = 1 then ls := [op(ls), Power(r, k) mod p] end if
    end do;
```

(7)

```
    return ls
end proc
```

Construct the list of all primitive roots for p = 29, 31 and 37 and count the number of elements in each list.

```
> L1 := allprimroots(29); L2 := allprimroots(31); L3 := allprimroots(37);
```

$$L1 := [2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15]$$

$$L2 := [3, 17, 13, 24, 22, 12, 11, 21]$$

$$L3 := [2, 32, 17, 13, 15, 18, 35, 5, 20, 24, 22, 19] \quad \textbf{(8)}$$

We compute the number of elements in each list as follows:

```
> nops(L1), nops(L2), nops(L3);
```

$$12, 8, 12 \quad \textbf{(9)}$$

Thus, lists L1 and L3 have 12 elements, whereas list L2 has 8. Note that these numbers are equal to phi(p-1) in each case (as expected).

```
> phi(29 − 1), phi(31 − 1), phi(37 − 1);
```

$$12, 8, 12 \quad \textbf{(10)}$$

```
>
```