```
> restart;
> interface(warnlevel = 0) :          # Maple 12
```

This worksheet has examples of prime number factorization. It uses the text procedure of finding the period and Euclid greatest common divisor algorithm. Also, we will use Maple's ifactor() and ifactors() functions. The ifactors() function returns the result in the following format

$$[u, [[p[1], e[1]], \ldots, [p[n], e[n]]]]$$

where $N = u(p[1]^{e[1]}) \ldots (p[n]^{e[n]})$,
p[i] is a prime integer,
e[i] is its exponent (multiplicity)
u is the sign of n.

for example:

$$-120 = -(2)^3\ (3)\ (5) \equiv [-1, [[2, 3], [3, 1], [5, 1]]]$$
$$120 = \ (2)^3\ (3)\ (5) \equiv [1, [[2, 3], [3, 1], [5, 1]]]$$

List of numbers to be factored

```
> L := [29143, 33389, 29747, 35263, 34933, 22487, 38021, 107143, 121879, 2045717] :
```

This is a large number whose prime factors are to be detremined using ifactor() and ifactors()

```
> BigNumber := 886564491457831264657084272587303954482637104140013743 31;
  print( This number has, length(BigNumber) digits );
```

BigNumber := 886564491457831264657084272587303954482637104140013743 31

This number has, 56 *digits* **(1)**

Euclid greatest common divisor algorithm; non-recursive

```
> Egcd2 := proc (a, b)
             local temp, x, y;
              x := a : y := b :
             while y <> 0 do
                   temp := y;
                    y := x mod y;
                     x := temp
              end do;
           end proc :
```

Period finding procedure

The procedure period is a very simple procedure which returns the period P from $a^P \bmod N = 1$ for small N. The procedure period(a,N) returns the period P or N if the period is not found.

```
> period := proc(a, N)
            local i, t;
            for i from 1 to N − 1 do
              t := a^i mod N;
              if t = 1 then return i end if;
            end do ;
            return N;
           end proc:
```

Factoring the list of numbers using period() and Egcd2()

```
> for i from 1 to 10 do
    N := L[i];   st := time( ) :
    Period := period(2, N);
    pf1 := Egcd2(2^(Period/2) + 1, N);
    pf2 := Egcd2(2^(Period/2) - 1, N);
    print((time( ) - st), seconds);   print( );
  end do;
```

$N := 29143$
$st := 1.201$
$Period := 480$
$pf1 := 193$
$pf2 := 151$
0., *seconds*

$N := 33389$
$st := 1.201$
$Period := 4128$
$pf1 := 193$
$pf2 := 173$
0.047, *seconds*

$N := 29747$
$st := 1.248$
$Period := 2940$
$pf1 := 197$
$pf2 := 151$
0.015, *seconds*

$N := 35263$
$st := 1.263$
$Period := 17444$
$pf1 := 197$
$pf2 := 179$
0.375, *seconds*

$N := 34933$
$st := 1.638$
$Period := 1440$
$pf1 := 193$
$pf2 := 181$
0.015, *seconds*

N := 22487
st := 1.669
Period := 2772
pf1 := 113
pf2 := 199
0.031, *seconds*

N := 38021
st := 1.700
Period := 4704
pf1 := 193
pf2 := 197
0.078, *seconds*

N := 107143
st := 1.778
Period := 5916
pf1 := 349
pf2 := 307
0.062, *seconds*

N := 121879
st := 1.840
Period := 2244
pf1 := 397
pf2 := 307
0.016, *seconds*

N := 2045717
st := 1.856
Period := 145914
pf1 := 1163
pf2 := 1759
14.773, *seconds*

(2)

Factoring the list of numbers using ifactor()

```
> for i from 1 to 10 do
    N := L[i];
    st := time( ) :
    ifactor(N);
    print( (time( ) − st), seconds);
    print( );
  end do;
```

$N := 29143$
$st := 16.754$
$(151)\,(193)$
$0.,\ seconds$

$N := 33389$
$st := 16.754$
$(173)\,(193)$
$0.,\ seconds$

$N := 29747$
$st := 16.754$
$(151)\,(197)$
$0.,\ seconds$

$N := 35263$
$st := 16.754$
$(179)\,(197)$
$0.,\ seconds$

$N := 34933$
$st := 16.754$
$(181)\,(193)$
$0.,\ seconds$

$N := 22487$
$st := 16.754$
$(113)\,(199)$
$0.,\ seconds$

$N := 38021$
$st := 16.754$
$(193)\,(197)$
$0.,\ seconds$

$N := 107143$
$st := 16.754$
$(307)(349)$
$0.$, *seconds*

$N := 121879$
$st := 16.754$
$(307)(397)$
$0.$, *seconds*

$N := 2045717$
$st := 16.754$
$(1163)(1759)$
$0.$, *seconds*

(3)

Factoring the BigNumber into prime factors using ifactor() and ifactors()

```
> st := time( ) :
  ifactor(BigNumber);
  st := time( ) − st :
  print(st, seconds);
  L2 := ifactors(BigNumber);
  pf1 := (L2[2, 1, 1]);
  if isprime(pf1) then print(It is a prime number with, length(pf1) digits) end if;
  pf2 := (L2[2, 2, 1]);
  if isprime(pf2) then print(It is a prime number with, length(pf2) digits) end if;
```

$(48215910563832798697)(183873846016889600127566887259284192 3)$
17.675, *seconds*
$L2 := [1, [[48215910563832798697, 1], [183873846016889600127566887259284192 3, 1]]]$
$pf1 := 48215910563832798697$
It is a prime number with, 20 *digits*
$pf2 := 183873846016889600127566887259284192 3$
It is a prime number with, 37 *digits*

(4)