```
> (* Mantej Sokhi *)
```

QUESTION 2B:

```
> restart:
> COMPUTERECPOL := proc(paramA::polynom)
  local temp,n,recPol:

  temp := paramA:
  n := degree(temp,x):
  recPol := expand(x^n*subs(x=1/x,temp)):

  return recPol:
  end proc:
> FINDINV := proc(f,x,n::posint,p)
  local yIN,y,k,temp;

  yIN := Rem(f mod p,x,x) mod p;
  if yIN=0 then
     error "FAIL":
  fi:
  y := (1/yIN) mod p;
  k := 1;

  while k<n do
     k := min(2*k, n);
    temp := Expand(f*y) mod p:
    y := Expand(y*(2-temp)) mod p:
    y := convert(taylor(y,x,k),polynom):
  od:

  return y:
  end proc:
> FASTQUO := proc(paramA::polynom,paramB::polynom,x,paramC::prime)
  local A,B,p,recPolA,recPolB,bInv,n,qRec,q:

  A := paramA:
  B := paramB:
  p := paramC:
  n := degree(A,x)-degree(B,x)+1:

  recPolA := COMPUTERECPOL(A):
  recPolB := COMPUTERECPOL(B):
```

```
  bInv := FINDINV(recPolB,x,n,p):

  qRec := Expand(bInv*recPolA) mod p:
  qRec := convert(taylor(qRec,x,n),polynom):
  q := Expand(x^(n-1)*subs(x=1/x,qRec)) mod p;

  return q:
  end proc:
> p := 9973:
  d := 1000:
> while d<10^5 do:
     a := Randpoly(2*d-1,x) mod p:
     b := Randpoly(d,x) mod p:
     q := CodeTools[Usage](FASTQUO(a,b,x,p)):
     if q<>Quo(a,b,x) mod p then
        print(BUG):
      fi:
     d := 2*d:
  od:
memory used=1.78MiB, alloc change=0 bytes, cpu time=9.00ms, real
time=10.00ms, gc time=0ns
memory used=3.39MiB, alloc change=0.81MiB, cpu time=18.00ms, real
time=19.00ms, gc time=0ns
memory used=7.12MiB, alloc change=5.55MiB, cpu time=38.00ms, real
time=38.00ms, gc time=0ns
memory used=15.46MiB, alloc change=2.36MiB, cpu time=83.00ms, real
time=83.00ms, gc time=3.72ms
memory used=31.86MiB, alloc change=43.58MiB, cpu time=201.00ms, real
time=202.00ms, gc time=14.85ms
memory used=65.64MiB, alloc change=6.41MiB, cpu time=393.00ms, real
time=383.00ms, gc time=29.20ms
memory used=135.16MiB, alloc change=7.42MiB, cpu time=1.09s, real
time=960.00ms, gc time=286.03ms
```