Assignment 2 Question 3(a) Wang's Rational Number Reconstruction

```
> WangsRNR := proc(a::integer,m::posint,N::posint,D::posint)
  local r,s,t,q,k;

     if 2*N*D >= m then error "bounds N,D too big" fi;
     r[0],r[1] := m,a mod m;
     s[0],s[1] := 1,0;
     t[0],t[1] := 0,1;
     k := 1;
     while r[k]>N do
        q := iquo(r[k-1],r[k]);
        r[k+1] := r[k-1]-q*r[k];
        s[k+1] := s[k-1]-q*s[k];
        t[k+1] := t[k-1]-q*t[k];
        k := k+1;
     od;
     # We have s[k] m + t[k] a = r[k]
     # ==>  t[k] a == r[k] mod m
     # ==>  a == r[k]/t[k] mod m if gcd(t[k],m)=1
     if abs(t[k])<=D and igcd(t[k],m)=1 then r[k]/t[k] else FAIL fi;

  end:
```

```
> m := 35;
  [seq( WangsRNR(i,m,4,4), i=0..m-1 )];
```

$$m := 35$$

$$\left[0, 1, 2, 3, 4, FAIL, FAIL, FAIL, -\frac{3}{4}, \frac{1}{4}, FAIL, -\frac{2}{3}, \frac{1}{3}, \frac{4}{3}, FAIL, FAIL, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \right. \quad (1)$$

$$\left. FAIL, FAIL, -\frac{4}{3}, -\frac{1}{3}, \frac{2}{3}, FAIL, -\frac{1}{4}, \frac{3}{4}, FAIL, FAIL, FAIL, -4, -3, -2, -1\right]$$