Assignment 3
CS 9566A

Paul Vrbik
250389673

November 4, 2009

Question 1 - Extended Euclidean Algorithm

Extended Euclidean Algorithm

```
EEA:=proc(a,b,x)
local n,u,c,d,c1,c2,d1,d2,r1,r2,r,q,g,s,t:

    n:=f->f/lcoeff(f,x):
    u:=f->lcoeff(f,x):

    c,d:=n(a),n(b):

    c1:=1:  c2:=0:  d1:=0:  d2:=1:

    for i from 0 while (d<>0) do
        q:=quo(c,d,x): r:=expand(c-q*d):
        r1:=expand(c1-q*d1): r2:=expand(c2-q*d2):
        c:=d: c1:=d1: c2:=d2:
        d:=r: d1:=r1: d2:=r2:
    end do:

    g:=n(c):
    s:=c1/(u(a)*u(c)):
    t:=c2/(u(b)*u(c)):

    return g,s,t:

end proc:
```

```
[>A1:=1-x+x^2:
[>A1:=1-x+x^2:
[>#check maple's EEA first.
[>r:=gcdex(A0,A1,x,'s','t'):
[>r,s,t;
```

$$1, 1/3, -x/3$$

```
[>#check my own code.
[>r,s,t:=EEA(A0,A1,x):
[>r,s,t;
```

$$1, 1/3, -x/3$$

```
[>expand(s*A0+t*A1) = r;
```

$$1 = 1$$

Table 1: Steps of the "Traditional Extended Euclidean Algorithm" (ALGORITHM 3.6 of Modern Computer Algebra)

i	q_i	r_i	s_i	t_i
0		$3+x-x^2+x^2$	1	0
1	x	$1-x+x^2$	0	1
2	$\frac{1}{3}-\frac{1}{3}x+\frac{1}{3}x^2$	3	1	$-x$
3		0	$\frac{1}{3}-\frac{1}{3}x+\frac{1}{3}x^2$	$1+\frac{1}{3}x-\frac{1}{3}x^2+\frac{1}{3}x^3$

Question 2 - The Golden Ratio

The *golden ratio* is $\varphi = (1+\sqrt{5})/2$.

(a) Find a polynomial $P \in \mathbb{Q}[x]$ of degree 2 such that $P(\varphi) = 0$. Letting $x = \varphi$ we do

$$x = \frac{1+\sqrt{5}}{2} \Rightarrow 2x = 1+\sqrt{5} \Rightarrow (2x-1) = \sqrt{5} \Rightarrow (2x-1)^2 = 5 \Rightarrow 4x^2-4x-4 = 0.$$

Thus by design $P(x) = 4x^2 - 4x - 4$ will have φ as a root; that is $P(\varphi) = 0$.

(b) Using XGCD we determine that

$$\frac{3-x}{5} \equiv \frac{1}{(x+2)} \bmod P(x).$$

This means

$$\frac{(3-x)(x-1)}{5} = \frac{-x^2+4x-3}{5} \equiv \frac{(x-1)}{(x+2)} \bmod P(x)$$

and using EUCLIDEAN DIVISION we can reduce $-x^2+4x-3 \bmod P$ giving:

$$\frac{3x-4}{5} \equiv \frac{(x-1)}{(x+2)} \bmod P(x).$$

implying (see Question 2c):

$$-\frac{4}{5} + \frac{3}{5}\varphi = \frac{\varphi - 1}{\varphi + 2}.$$

Don't believe me?

```
[>phi:=(1+sqrt(5))/2:
[>simplify( (3*phi/5-4/5) - (phi-1)/(phi+2) );
```

$$0$$

(c) For any fraction X in φ assume that we have $f, g \in \mathbb{Q}[x]$ such that $X = f(\varphi)/g(\varphi)$. Provided that:

1. the fraction f/g is reduced (otherwise use GCD and EUCLIDEAN DIVISION to remove the common factor)
2. $g(\varphi) \neq 0$ (which is an implicit assumption but I want to make it *explicit*)

I *can* do this with more general fractions in φ. (Note for the case where $f = g$ or $f(\varphi) = 0$ that the desired decomposition is 1 and 0 respectively).

First observe that the inverse of g mod P exists. As $P(x)$ is irreducible (it is straightforward to show it has no linear factors in $\mathbb{Q}[x]$) $\gcd(g, P) \neq 1 \Rightarrow P \big| \gcd(g, P) \Rightarrow g(\varphi) = 0$, a contradiction. Therefore $\gcd(g, P) = 1$ which implies the inverse g mod P exists (by XGCD).

Following the scheme in Question 2b we can use XGCD and EUCLIDEAN DIVISION to find a_0, a_1 such that

$$a_0 + a_1 x \equiv \frac{f(x)}{g(x)} \bmod P \tag{1}$$

(as P is degree two everything in the quotient ring $\mathbb{Q}[x]/\langle P\rangle$ will be a linear function in x).

Equation (1) implies

$$\frac{f(x)}{g(x)} = (a_0 + a_1 x) + Q(x)P(x)$$

where $Q(x) = \mathrm{quo}(f \cdot (g^{-1} \bmod P), P, x)$ which further implies

$$\frac{f(\varphi)}{g(\varphi)} = (a_0 + a_1\varphi) + Q(\varphi)P(\varphi) = a_0 + a_1\varphi$$

as desired.

Question 3 - Rational Reconstruction and Sequences

Rational Reconstruction

```
myRatRecon:=proc(G,x)
local Uo, Vo, Ao, Up, Vp, Ap, i, Q;

    Uo:=1;  Vo:=0;  Ao:=x^(degree(G,x)+1);
    Up:=0;  Vp:=1;  Ap:=G;

    for i from 1 while Ap<>0 do
        Q:=expand( quo( Ao,Ap,x ) );
        Ao, Ap := Ap, expand( Ao-Q*Ap );
        Uo, Up := Up, expand( Uo-Q*Up );
        Vo, Vp := Vp, expand( Vo-Q*Vp );
    end do;

    return simplify(Ao/Vo);

end proc:
```

From slide "Proof on an example" we have that all recurrences of order two with $u_0 = \alpha$, $u_1 = \beta$ and $u_{n+2} + au_{n+1} + bu_n = 0$ satisfy

$$S = \frac{\alpha + (\beta + \alpha a)\, x}{1 + ax + bx^2}. \tag{2}$$

We are given the sequence $u_i = (i+1)$ for $i \leq 0 \leq 10$ for which the sum S satisfies

$$S = \sum_{i \geq 0} u_i x^i \equiv \frac{1}{1-2x+x^2} \mod x^{10}$$

which we determine using `myRatRecon` as follows:

```
[>f:=add( (i+1)*x^i, i=0..9);
```

$$f := 1 + 2x^2 + 3x^3 + 4x^3 + 5x^5 + 6x^6 + 7x^7 + 8x^8 + 9x^9 + 10x^{10}$$

```
[>myRatRecon(f,x);
```

$$\frac{1}{1-2x+x^2}$$

Therefore by (2) we have

$$\frac{1}{1-2x+x^2} = \frac{\alpha + (\beta + \alpha a)\, x}{1+ax+bx^2} = \frac{1}{1+ax+bx^2}$$

implying $a = -2$, $b = 1$ giving the order two recurrence defined by:

$$u_0 = \alpha, \qquad u_1 = \beta, \qquad u_{n+2} - 2u_{n+1} + u_n = 0.$$

We can check if this is the correct answer in MAPLE:

```
[>u:=n->2*u(n-1)-u(n-2):
[>u(0):=1: u(1):=2:
[>seq( u(i), i=0..9 );
```

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$$

Question 4

For the given sequences a_i and v_i, let $Q(x) \in \mathbb{Q}[x]$ be degree less than n such that $Q(a_i) = v_i$ for all i and $M(x) = (x - a_1) \cdots (x - a_n)$. We can run XGCD with inputs Q and M.

$(U_0, V_0, A_0) \leftarrow (1, 0, M)$;
$(U_1, V_1, A_1) \leftarrow (0, 1, Q)$;
for $i \geq 2$ **do**
  $Q_i \leftarrow \text{quo}(A_{i-1}, A_i, x)$;
  $A_{i+1} \leftarrow A_{i-1} - Q_i A_i$;
  $U_{i+1} \leftarrow U_{i-1} - Q_i U_i$;
  $V_{i+1} \leftarrow V_{i-1} - Q_i V_i$;
end for

At each step we maintain the invariant

$$U_i M + V_i Q = A_i \tag{3}$$

and moreover the degrees of the of A_i and V_i decrease and increase (respectively) from $\deg(Q) = n$ and 0. Therefore if we let i be the first index where $\deg(A_i) \leq n/2$ then $\deg(V_i) = n - \deg(A_{i-1}) \leq n/2$ (guaranteed by well-ordering principle). By re-arranging (3) we get the desired result, notice:

$$\begin{aligned} U_i(x)M(x) + V_i(x)Q(x) = A_i(x) &\Rightarrow Q(x) = \frac{A_i(x) - U_i(x)M(x)}{V_i(x)} \\ &\Rightarrow Q(a_i) = \frac{A_i(a_i) - U_i(a_i)M(a_i)}{V_i(a_i)} \text{ for every } i \\ &\Rightarrow Q(a_i) = \frac{A_i(a_i) - 0}{V_i(a_i)} \\ &\Rightarrow v_i = \frac{A_i(a_i)}{V_i(a_i)} \end{aligned}$$

Letting $A_i = N$ and $V_i = D$ we have found $P = N/D$ such that $P(a_i) = N(a_i)/D(a_i) = v_i$ for every i. Moreover, by our design, $\deg N, \deg D \leq n/2$. Thus we have constructed P with the necessary requirements.

To make this proof complete the following would have to be shown:

1. *That the invariant (3) is true (non-trivial)*
2. *That the degrees of A_i and V_i form (respectively) strictly decreasing and increasing sequences for which the degrees decrease/increase by one each step.*

Question 5

time to complete $\approx$ 5 hours

(plus a whole bunch of "wasted" time figuring out the best way to represent Maple listings and worksheets in LaTeX.)