Assignment 2 Question 4: Chinese Remaindering

Part (a)

```
> restart;
  u1,m1 := 3,5;
```

$$u1, m1 := 3, 5$$

```
> u2,m2 := 1,7;
```

$$u2, m2 := 1, 7$$

```
> u3,m3 := 3,9;
```

$$u3, m3 := 3, 9$$

The solution of $u \in \mathbb{Z}$ satisfying $u \equiv u_i \bmod m_i$ and $0 \le u < M$ where $M = m_1 \cdot m_2 \cdot m_3$ is

```
> chrem( [u1,u2,u3],[m1,m2,m3] );
```

$$183$$

For the mixed radix represenation you need so write $u = v_0 + v_1 \cdot m_1 + v_2 \cdot m_1 \cdot m_2$ and solve for v_0, v_1, v_2 .

```
> v0 := u1 mod m1;
```

$$v0 := 3$$

```
> i1 := m1^(-1) mod m2;
  v1 := (u2 - v0)*i1 mod m2;
```

$$i1 := 3$$

$$v1 := 1$$

```
> i1 := 1/m1 mod m3;
  i2 := 1/m2 mod m3;
  v2 := (u3-v0-v1*m1)*i1*i2 mod m3;
```

$$i1 := 2$$

$$i2 := 4$$

$$v2 := 5$$

```
> v0+v1*m1+v2*m1*m2;
```

$$183$$

For the Lagrange representation write $u = w_1 \cdot m_2 \cdot m_3 + w_2 \cdot m_1 \cdot m_3 + w_3 \cdot m_2 \cdot m_3$ and solve for w_1, w_2, w_3 .

```
> w1 := u1/(m2*m3) mod m1;
```

$$w1 := 1$$

```
> w2 := u2/(m1*m3) mod m2;
```

$$w2 := 5$$

```
> w3 := u3/(m1*m2) mod m3;
```

$$w3 := 6$$

```
> u := w1*m2*m3+w2*m1*m3+w3*m1*m2;
```

$$u := 498$$

You must reduce this mod M

```
> M := m1*m2*m3;
  u := modp(u,M);
```

$$M := 315$$

$$u := 183$$

Part (b)

Newton's method

```
> x1,x2,x3 := 0,1,2;
  y1,y2,y3 := 1,3,4;
```

$$x1, x2, x3 := 0, 1, 2$$

$$y1, y2, y3 := 1, 3, 4$$

```
> v0 := y1 mod 5;
  v1 := (y2-v0)/(x2-x1) mod 5;
  v2 := (y3-v0-v1*(x3-x1))/(x3-x1)/(x3-x2) mod 5;
```

$$v0 := 1$$

$$v1 := 2$$

$$v2 := 2$$

```
> f := v0+v1*(x-x1)+v2*(x-x1)*(x-x2);
```

$$f := 1 + 2\,x + 2\,x\,(x-1)$$

```
> seq( Eval(f,x=alpha) mod 5, alpha=[x1,x2,x3] );
```

$$1, 3, 4$$

Part (c)

```
> restart;
  a := (9*y-7)*x + (5*y^2+12);
```

$$a := (9\,y-7)\,x + 5\,y^2 + 12$$

```
> b := (13*y+23)*x^2 + (21*y-11)*x + (11*y-13);
```

$$b := (13\,y+23)\,x^2 + (21\,y-11)\,x + 11\,y - 13$$

Let $c = a\,b$. A simple bound for $||c||_\infty$ is to count the number of terms in a and b and take the minimum and multiply this by $||a||_\infty \cdot ||b||_\infty$. That is

```
> bound := 4 * 12 * 23;
```

$$bound := 1104$$

We require that the product of the primes $M > 2 \cdot ||c||_\infty$ so three primes 23,29,31 is good.

```
> P := [23,29,31];
  M := P[1]*P[2]*P[3];
```

$$P := [23, 29, 31]$$

$$M := 20677$$

To interpolate

```
> deg[y](c) = degree(a,y) + degree(b,y);
  deg[x](c) = degree(a,x) + degree(b,x);
```

$$deg[y](c) = 3$$

$$deg[x](c) = 3$$

The product will have degree 3 in y so we need 4 evaluation points to interpolate it. I'm using $\alpha = 0, 1, 2, 3$.
The product will have degree 3 in x so 4 evaluation points to interpolate it. I'm using $\beta = 0, 1, 2, 3$.

```
> Y := [0,1,2,3];
  X := [0,1,2,3];
```

$$Y := [0, 1, 2, 3]$$

$$X := [0, 1, 2, 3]$$

Iterate over the primes, for each prime over the evaluation points for y, for each evaluation point over the evaluation points for x.

```
> for i to nops(P) do
      p := P[i];
     A[p] := a mod p;
     B[p] := b mod p;
     Cy := Array(0..3);
     for alpha in Y do
        Ay[alpha] := Eval(A[p],y=alpha) mod p;
        By[alpha] := Eval(B[p],y=alpha) mod p;
         Cyx := Array(0..3);
         for beta in X do
            Ayx[beta] := Eval(Ay[alpha],x=beta) mod p;
            Byx[beta] := Eval(By[alpha],x=beta) mod p;
            Cyx[beta] := Ayx[beta]*Byx[beta] mod p;
          od;
        Cy[alpha] := Interp(X,Cyx,x) mod p;
      od;
     C[i] := Interp(Y,Cy,y) mod p;
  od:
  C[1];
```

$$(19 x^2 + 13 x + 9) y^3 + (2 x^3 + 5 x^2 + 21 x + 4) y^2 + (x^3 + 2 x^2 + 12 x + 17) y + 8 x^2 + 5 x + 5$$

Notice that the images are not expanded. Maple's chrem command likes them expanded.

```
> for i to nops(P) do C[i] := expand(C[i]) od:
> c := mods( chrem( [C[1],C[2],C[3]], P ), M );
```

$$c := 117 x^3 y^2 + 65 x^2 y^3 + 116 x^3 y + 304 x^2 y^2 + 105 x y^3 - 161 x^3 - 90 x^2 y + 44 x y^2 + 55 y^3 + 353 x^2 + 58 x y - 65 y^2 - 41 x + 132 y - 156$$

```
> expand( a*b );
```

$$117 x^3 y^2 + 65 x^2 y^3 + 116 x^3 y + 304 x^2 y^2 + 105 x y^3 - 161 x^3 - 90 x^2 y + 44 x y^2 + 55 y^3$$

$$+353x^2+58xy-65y^2-41x+132y-156$$

It worked!

> Part (c)