Assignment 3 Question 3

Part (a)

Let $A = a_n \cdot \prod_{i=1}^{n} x - \alpha_i$ and $B = b_m \cdot \prod_{i=1}^{m} \beta_i$. The defintion of the resultant is

$$res(A(x), B(x)) = a_n^m \cdot b_m^n \cdot \prod_{i=1}^{n} \cdot \prod_{j=1}^{m} \alpha_i - \beta_j .$$

```
> A := 3*x^2+3; n := 2;
  B := (x-2)*(x+5); m := 2;
```

$$A := 3x^2 + 3$$

$$n := 2$$

$$B := (x-2)(x+5)$$

$$m := 2$$

```
> alpha := solve(A,x);
```

$$\alpha := I, -I$$

```
> beta := solve(B,x);
```

$$\beta := -5, 2$$

```
> lcoeff(A)^m*lcoeff(B)^n*mul( mul( alpha[i]-beta[j], j=1..m ), i=1..n
  ) ;
```

$$1170$$

We should check it.

```
> resultant(A,B,x);
```

$$1170$$

Part (b)

If $C = c_l \cdot \prod_{i=1}^{l} x - \gamma_i$ then $B \cdot C = b_m \cdot c_l \cdot \prod_{j=1}^{m} (x - \beta_j) \cdot \prod_{k=1}^{l} (x - \gamma_k)$ so using the definition we have

$$res(A, B \cdot C) = a_n^{m+l} \cdot (b_m \cdot c_l)^n \cdot \prod_{i=1}^{n} \left[\prod_{j=1}^{m} (\alpha_i - \beta_j) \cdot \prod_{k=1}^{l} (\alpha_i - \gamma_k) \right]$$

$$= a_n^m \cdot b_m^n \cdot \left[\prod_{i=1}^{n} \cdot \prod_{j=1}^{m} \alpha_i - \beta_j \right] \cdot a_n^l \cdot c_l^n \left[\prod_{i=1}^{n} \cdot \prod_{k=1}^{l} \alpha_i - \beta_k \right]$$

$$= res(A, B) \cdot res(A, C).$$

Part (c)

```
> A := 58*x^4-415*x^3-111*x+213;
```

$$A := 58x^4 - 415x^3 - 111x + 213$$

```
> B := 69*x^3-112*x^2+413*x+113;
```

$$B := 69\,x^3 - 112\,x^2 + 413\,x + 113$$

```
> G := gcd(A,B);
```

$$G := 1$$

So A and B are relatively prime. The unlucky primes are the primes which divide the resultant.

```
> R := resultant(A,B,x);
```

$$R := 232546626971939784$$

```
> ifactor(R);
```

$$(2)^3\,(3)\,(7)\,(196648119467)\,(7039)$$

So we have unlucky primes 2,3,7,7039,196648119467. Let's check them.

```
> for p in [2,3,7,7039,196648119467] do
    Gcd(A,B) mod p;
  od;
```

$$x^3 + x + 1$$

$$x + 2$$

$$x + 5$$

$$x + 5407$$

$$x + 51402852970$$

We could do that by factoring them modulo p

```
> Factor(A) mod p;
```

$$58\,(x^2 + 4657091945\,x + 61620628281)\,(x + 51402852970)\,(x + 184664477184)$$

```
> Factor(B) mod p;
```

$$69\,(x^2 + 99645702561\,x + 88696325121)\,(x + 51402852970)$$