The Modular Gcd Algorithm

```
> a := 8*x^4+78*x^3+166*x^2-171*x-360;
  b := 12*x^5+84*x^4+90*x^3-2*x^2-14*x-15;
```

$$a := 8x^4 + 78x^3 + 166x^2 - 171x - 360$$

$$b := 12x^5 + 84x^4 + 90x^3 - 2x^2 - 14x - 15 \quad (1)$$

```
> content(a,x), content(b,x);
```

$$1, 1 \quad (2)$$

```
> MignotteBound := proc(f,x) local d;
     d := degree(f,x); 2^d*ceil(sqrt(d+1))*maxnorm(f) end:
> B := min( MignotteBound(a,x), MignotteBound(b,x) );
```

$$B := 8640 \quad (3)$$

```
> M := 23*29*31;
```

$$M := 20677 \quad (4)$$

```
> gamma := igcd(lcoeff(a),lcoeff(b));
```

Error, attempting to assign to `gamma` which is protected. Try declaring `local gamma`; see ?protect for details.

```
> beta := igcd(lcoeff(a),lcoeff(b));
```

$$\beta := 4 \quad (5)$$

```
> g1 := Gcd(a,b) mod 23;
  g1 := beta*g1 mod 23;
```

$$g1 := x^2 + 7x + 19$$

$$g1 := 4x^2 + 5x + 7 \quad (6)$$

```
> g2 := Gcd(a,b) mod 29;
  g2 := beta*g2 mod 29;
```

$$g2 := x^2 + 7x + 22$$

$$g2 := 4x^2 + 28x + 1 \quad (7)$$

```
> g3 := Gcd(a,b) mod 31;
  g3 := beta*g3 mod 31;
```

$$g3 := x^2 + 7x + 23$$

$$g3 := 4x^2 + 28x + 30 \quad (8)$$

```
> gbar := mods( chrem([g1,g2,g3],[23,29,31]), M );
```

$$gbar := 4x^2 + 28x + 30 \quad (9)$$

```
> g := primpart(gbar);
```

$$g := 2x^2 + 14x + 15 \quad (10)$$

```
> divide(a,g), divide(b,g);
```

$$true, true \quad (11)$$

```
> infolevel[gcd] := 4:
  gcd(a,b);
gcd/gcdchrem1: computing images
gcd/gcdchrem1: combining images
gcd/gcdchrem1: trial division
```

$$2x^2 + 14x + 15 \quad (12)$$