Assignment 1 Question 4

Copyright, Michael Monagan, September 2023.

Part (a)

```
> a,b := 99,28;
```

$$a, b := 99, 28 \tag{1}$$

```
> r[0],r[1] := a,b;
  s[0],s[1] := 1,0;
  t[0],t[1] := 0,1;
  k := 1;
  printf("    k   r[k]   q[k]   s[k]   t[k]\n");
  while r[k]<>0 and k<10 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;
     printf("%6d   %4d   %4d   %4d   %4d\n",k,r[k],q,s[k],t[k]);
  od:
```

$$r_0, r_1 := 99, 28$$

$$s_0, s_1 := 1, 0$$

$$t_0, t_1 := 0, 1$$

$$k := 1$$

k	r[k]	q[k]	s[k]	t[k]
2	15	3	1	−3
3	13	1	−1	4
4	2	1	2	−7
5	1	6	−13	46
6	0	2	28	−99

Thus the gcd of a and b is 1 and the inverse of b mod a is 46.

```
> 1/b mod a;
```

$$46 \tag{2}$$

Parts (b)

```
> a,b := 1234,4321;
```

$$a, b := 1234, 4321 \tag{3}$$

```
> igcdex(a,b,'s','t');
```

$$1 \tag{4}$$

```
> s,t;
```

$$-1082, 309 \tag{5}$$

```
> s*a+t*b;
```

$$1 \tag{6}$$

The inverse of a mod b is s = -1028. We want the inverse in the range [0,b) so let's add b to s

```
> s+b;
```

$$3239 \quad \textbf{(7)}$$

```
> 1/a mod b;
```

$$3239 \quad \textbf{(8)}$$

Part (c)

```
> a,b := x^3-1,x^4-1;
```

$$a, b := x^3 - 1, x^4 - 1 \quad \textbf{(9)}$$

```
> g := gcdex(a,b,x,'s','t');
```

$$g := x - 1 \quad \textbf{(10)}$$

```
> s,t;
```

$$-x, 1 \quad \textbf{(11)}$$

Let's check s a + t b = g

```
> s*a+t*b;
```

$$-\left(x^3 - 1\right) x + x^4 - 1 \quad \textbf{(12)}$$

```
> expand(s*a+t*b);
```

$$x - 1 \quad \textbf{(13)}$$