```
> (-1)*11^(-1) mod 16;
```

$$13 \tag{1}$$

```
>
> 11*13;
>
```

$$143 \tag{2}$$

```
>
> convert(143,binary);
```

$$10001111 \tag{3}$$

```
>
> mult:=proc(p,s)
  local x,y,k;
  y:=s mod 2^p;
  x:=(-1)*y^(-1) mod 2^p;
  k:=0;
  while 2^k<x*y do k:=k+1;od;
  print (pprime=k);
  return [convert(x*y-1,binary),convert(x*y+1,binary)];
  end proc;
```

proc(p, s) (4)

local x, y, k;
$y := mod(s, 2\hat{}p)$;
$x := mod(-1/y, 2\hat{}p)$;
$k := 0$;
while $2\hat{}k < x*y$ **do** $k := k+1$ **end do**;
$print(pprime = k)$;
return $[convert(x*y-1, binary), convert(x*y+1, binary)]$
end proc

```
> mult(4,11);
```

$$pprime = 8$$
$$[10001110, 10010000] \tag{5}$$

```
> mult(5,13);
>
```

$$pprime = 9$$
$$[101011110, 101100000] \tag{6}$$

```
> mult(3,5);
```

$$pprime = 4$$
$$[1110, 10000] \tag{7}$$

```
> mult(10,113);
```

$$pprime = 17$$
$$[11000001111111110, 11000010000000000] \tag{8}$$

```
> 5^(-1) mod 2^5;
```

$$13 \tag{9}$$

```
> racine :=proc(p, k)
  local l, x, y, i;
  l := 3;
  x := [1, 3, 0, 0];
  while l < p do
    for i from 1 to 2 do
      y[i] := (x[i])^(-1) mod 2^(2·l-1);
```

```
        x[i] := (x[i] + k·y[i])/2 mod 2^l;
      od;
      l := 2·l − 2;
    od;
    for i from 1 to 2 do
        y[i] := (x[i])^(−1) mod 2^(2·l − 1);
        x[i] := (x[i] + k·y[i])/2 mod 2^(p−1);
        x[i + 2] := −x[i] mod 2^p;
      od;
    return x;
    end proc;
```

(10)

```
proc(p, k)
    local l, x, y, i;
    l := 3;
    x := [1, 3, 0, 0];
    while l < p do
        for i to 2 do
            y[i] := mod(1/x[i], 2^(2*l − 1)); x[i] := mod(1/2*x[i] + 1/2*k*y[i], 2
            ^l)
        end do;
        l := 2*l − 2
    end do;
    for i to 2 do
        y[i] := mod(1/x[i], 2^(2*l − 1));
        x[i] := mod(1/2*x[i] + 1/2*k*y[i], 2^(p − 1));
        x[i + 2] := mod(−x[i], 2^p)
    end do;
    return x
end proc
```

(11)

```
> debug(racine); racine(6, 1);
```

racine

```
{--> enter racine, args = 6, 1
```

3

[1, 3, 0, 0]

1

1

11

7

4

1

1

55

15

6

1

1

63

1775

31

33

```
<-- exit racine (now at top level) = [1, 31, 63, 33]}
```

$$[1, 31, 63, 33]$$

```
> x := %;
```

$$[3581, 3075, 1021, 515] \quad \textbf{(12)}$$

```
> 29^2 mod 2^6;
```

$$9 \quad \textbf{(13)}$$

```
> `?`
```