```
> x_adic := proc(input_a, u0, p)
    local a,k,u,d, ek,t,uk;
    a := input_a;
    k := 1;
    u := u0;
    d := -2*u;
    while true do
        Rem(a-u^2, x^k, x) mod p;
        ek := expand(a - u^2) mod p;
        if ek = 0 then return u; fi;
        if k > degree(a) / 2 then return FAIL; fi;
        t := -expand(ek/x^k);
        Divide(Rem(t, x, x), d, 'q') mod p;
        uk := q;
        u := u + uk*(x^k);
        printf("u%d = %a\n", k, u);
        k := k + 1;
    od;
  end;
```

```
x_adic := proc(input_a, u0, p)                                        (1)
    local a, k, u, d, ek, t, uk;
    a := input_a;
    k := 1;
    u := u0;
    d := -2*u;
    do
        Rem(a - u^2, x^k, x) mod p;
        ek := expand(a - u^2) mod p;
        if ek = 0 then return u end if;
        if 1/2*degree(a) < k then return FAIL end if;
        t := -expand(ek/x^k);
        Divide(Rem(t, x, x), d, 'q') mod p;
        uk := q;
        u := u + uk*x^k;
        printf("u%d = %a\n", k, u);
        k := k + 1
    end do
end proc
```

```
> a1 := 81*x^6+ 16*x^5+ 24*x^4+ 89*x^3+ 72*x^2+ 41*x+ 25;
  a2 := 81*x^6+ 46*x^5+ 34*x^4+ 19*x^3+ 72*x^2+ 41*x+ 25;
  p := 101;
  u0 := 5;
  Rem(a1-u0^2, x, x) mod p;
```

$$a1 := 81\,x^6 + 16\,x^5 + 24\,x^4 + 89\,x^3 + 72\,x^2 + 41\,x + 25$$

$$a2 := 81\,x^6 + 46\,x^5 + 34\,x^4 + 19\,x^3 + 72\,x^2 + 41\,x + 25$$

$$p := 101$$

$$u0 := 5$$

(2)

$$0 \qquad (2)$$

```
> u := x_adic(a1, u0, p);
u1 = 5+95*x
u2 = 44*x^2+95*x+5
u3 = 92*x^3+44*x^2+95*x+5
```

$$u := 92\,x^3 + 44\,x^2 + 95\,x + 5 \qquad (3)$$

```
> expand(a1 - u^2) mod p
```

$$0 \qquad (4)$$

```
> u := x_adic(a2, u0, p);
u1 = 5+95*x
u2 = 44*x^2+95*x+5
u3 = 85*x^3+44*x^2+95*x+5
```

$$u := \mathit{FAIL} \qquad (5)$$