```
> MY_ZSQRT := proc(a,u0,p) local  u, prev_u, pk, prev_pk, prev_pk_2
  ,k,e,prev_e, ekpk, prev_ekpk, uk, prev_uk, i;
      u := mods(u0,p);
      i := modp(1/(2*u0),p);
      pk := p;
      prev_pk_2 := 1;
      for k do
          if k <= 1 then
             ekpk := iquo(a-u^2, pk);
          else
             prev_ekpk := ekpk;
             ekpk := iquo(prev_ekpk - 2*prev_u*prev_uk, p) -
  prev_uk*prev_uk*prev_pk_2;
          fi;
          if ekpk = 0 then return(u); fi;
          if ekpk < 0 then return(FAIL) fi;

          if k <= 1 then
              uk :=  mods(ekpk*i, p);
          else
              prev_ekpk := ekpk;
              uk := mods(ekpk*i, p);
              prev_pk_2 := prev_pk_2*p;
          fi;

          # printf("uk is %a, prev_nk is %a \n", uk, prev_uk);
          prev_uk := uk;
          prev_u := u;
          prev_pk := pk;
          u := u + uk*pk;
          pk := p*pk;
      od;
  end:
> ZSQRT := proc(a,u0,p) local u,pk,k,e,uk,i;
      u := mods(u0,p);
      i := modp(1/(2*u0),p);
      pk := p;for k do
          e := a - u^2;
          if e = 0 then return(u); fi;
          if e < 0 then return(FAIL) fi;
          uk :=  mods( iquo(e,pk)*i, p );
          # printf("uk is %a \n", uk);
          u := u + uk*pk;
          pk := p*pk;
      od;
  end:
> p :=9973;
```

$$p := 9973 \tag{1}$$

```
> ###################### Original ZSQRT ######################
> a := 3^20000:
  u0 := 3^10000 mod p;
  t1 := time(ZSQRT(a, u0, p));
```

$$u0 := 7888$$
$$t1 := 0.089 \tag{2}$$

```
> a := a*a: u0 := u0*u0 mod p:
  t2 := time(ZSQRT(a, u0, p)); t2/t1;
```

$$t2 := 0.702$$

$$3.943820225 \quad (3)$$

```
> a := a*a: u0 := u0*u0 mod p:
  t3 := time(ZSQRT(a, u0, p)); t3/t2;
```

$$t3 := 3.871$$

$$5.514245014 \quad (4)$$

```
> a := a*a: u0 := u0*u0 mod p:
  t4 := time(ZSQRT(a, u0, p)); t4/t3;
```

$$t4 := 19.858$$

$$5.129940584 \quad (5)$$

```
> a := a*a: u0 := u0*u0 mod p:
  t5 := time(ZSQRT(a, u0, p)); t5/t4;
```

$$t5 := 87.151$$

$$4.388709840 \quad (6)$$

```
> ###################### Modified ZSQRT ######################
> a := 3^20000:
  u0 := 3^10000 mod p;
  t1 := time(MY_ZSQRT(a, u0, p));
```

$$u0 := 7888$$

$$t1 := 0.121 \quad (7)$$

```
> a := a*a: u0 := u0*u0 mod p:
  t2 := time(MY_ZSQRT(a, u0, p)); t2/t1;
```

$$t2 := 0.347$$

$$2.867768595 \quad (8)$$

```
> a := a*a: u0 := u0*u0 mod p:
  t3 := time(MY_ZSQRT(a, u0, p)); t3/t2;
```

$$t3 := 1.633$$

$$4.706051873 \quad (9)$$

```
> a := a*a: u0 := u0*u0 mod p:
  t4 := time(MY_ZSQRT(a, u0, p)); t4/t3;
```

$$t4 := 6.093$$

$$3.731169626 \quad (10)$$

```
> a := a*a: u0 := u0*u0 mod p:
  t5 := time(MY_ZSQRT(a, u0, p)); t5/t4;
```

$$t5 := 23.657$$

$$3.882652224 \quad (11)$$

```
> a := a*a: u0 := u0*u0 mod p:
  t6 := time(MY_ZSQRT(a, u0, p)); t6/t5;
```

$$t6 := 93.890$$

$$3.968804159 \quad (12)$$