Lec 14C Handouts

March 4, 2021 1:43 PM

Compute a 3-adic representation for 65 in the positive range

```
> U := 65;
  p := 3;
  for k from 0 while U <> 0 do
     u[k] := modp(U,p);
     U := iquo(U-u[k],p);
  od:
  n := k;
```

$$U := 65$$
$$p := 3$$
$$n := 4$$

```
> seq( u[k], k=0..n-1 );
  65 = add( u[k]*``(p)^k, k=0..n-1 );
```

$$2, 0, 1, 2$$
$$65 = 2 + (3)^2 + 2\,(3)^3$$

Using the symmetric range

```
> U := 65;
  p := 3;
  for k from 0 while U <> 0 do
     u[k] := mods(U,p);
     U := iquo(U-u[k],p);
  od:
  n := k;
```

$$U := 65$$
$$p := 3$$
$$n := 5$$

```
> seq( u[k], k=0..n-1 );
  65 = add( u[k]*``(p)^k, k=0..n-1 );
```

$$-1, 1, 1, -1, 1$$
$$65 = -1 + (3) + (3)^2 - (3)^3 + (3)^4$$

Algorithm P-adic$\sqrt{\ }$ (a, u_0, p, B)

Input $a \in \mathbb{Z}^+$

$p > 2$ prime.

$u_0 \in \mathbb{Z}$ s.t. $a - u_0^2 \equiv 0 \pmod p$

and $u_0 \not\equiv 0 \pmod p$

$B \geq \sqrt{a}$ a bound.

Output FAIL $\Rightarrow \sqrt{a} \notin \mathbb{Z}$ or $\sqrt{a}$

$u \leftarrow \text{mods}(u_0, p)$

$i \leftarrow 1/(2u_0) \bmod p$

for $k = 1, 2, 3, \ldots$ do

$e \leftarrow a - u^2$

if $e = 0$ then output u.

if $p^k > 2B$ then output FAIL

$e \leftarrow e/p^k$

$u_k \leftarrow \text{mod}\underline{\text{s}}(i \cdot e, p)$

$u \leftarrow u + u_k p^k$

end for

end.

Compute a sqrt in **Z** using a linear p-adic Newton iteration.

```
> NI := proc(u0::integer,a::posint,p::prime,B::posint) local u,e,uk,
  pk,k,i;
      u := mods(u0,p);
      i := (2*u0)^(-1) mod p;
      pk := p;
      k := 1;
      while true do
          e := a-u^2;
          if e=0 then return u; fi;
          if pk > 2*B then return FAIL; fi;
          e := iquo(e,pk) mod p;
          uk := mods(i*e,p);
          u := u + uk*pk;
          pk := p*pk;
      od;
  end:
> a := 131^2;
```

$$a := 17161$$

How can we reorganize this computation so that the cost is $O(n^2)$ instead of $O(n^3)$.

```
> p := 7;
```

$$p := 7$$

```
> Factor( x^2-a ) mod p;
```

$$(x+5)\ (x+2)$$

```
> NI(-2,a,p,200);
```

$$131$$

```
> NI(2,a,p,200);
```

$$-131$$

```
> p := prevprime(10^4):
> a := 3^20000: u0 := 3^10000 mod p:
> time(NI(u0,a,p,a));
```

$$0.109$$

```
> a := a*a: u0 := u0*u0 mod p:
> time(NI(u0,a,p,a));
```

$$0.380$$

```
> a := a*a: u0 := u0*u0 mod p:
> time(NI(u0,a,p,a));
```

$$2.300$$

```
> a := a*a: u0 := u0*u0 mod p:
> time(NI(u0,a,p,a));
```

$$11.452$$

p is a constant

for k from 1 to $\frac{n}{2}$ do $\quad O(k^2)$

$$\sum_{k=1}^{n/2} O(k^2) = O\left(\sum_{k=1}^{n/2} k^2\right) \in O(n^3)$$

$$\sum_{k=1}^{n} k^2 = \frac{n(2n+1)(n+1)}{6}$$

$\sqrt{a}$ $\quad a \in \mathbb{Z}[x]$

$\sqrt[3]{a(x)}$