2 -- cyclo linear algebra

```
def padic_cyclotomic_reconstruction(K, w, p, prec, phi):
   n = K.degree()
   zeta = K.gen()
   X = [zeta^i for i in range(n)] + [w]
   A = matrix(ZZ, n + 2, n + 2)
   for i in range(len(X)):
        A[i,i] = 1
        A[i,n+1] = Mod(phi(X[i]), p^prec).lift()
   A[n+1, n+1] = p^(prec-1)
   L = A.LLL()
   #print L
   rr = L[1].copy()
   rr[0] -= rr[-1]
   alpha = -1/rr[-2]
   lin_comb = rr[:-2]*alpha
   return K(lin_comb.list())

def solve_cyclo(A, v, prec=20, pstart=2^10):
   # solve A*x = v over cyclotomic number field
   K = A.base_ring()
   n = K.number_of_roots_of_unity()
   p = pstart
   while p % n != 1:
       p = next_prime(p)
   print "p = ", p
   f = K.defining_polynomial()
   C = pAdicField(p, prec)
   R = f.roots(C)
   phi = K.hom(QQ(R[0][0].lift()), check=False)
   B = matrix(QQ, A.nrows(), A.ncols(), [phi(w) for w in A.list()])
   z = matrix(QQ, v.nrows(), v.ncols(), [phi(w) for w in v.list()])
   #return B.change_ring(ZZ), z.change_ring(ZZ)
   #print B
   time xx = B.solve_right(z) % p^prec
   #print xx
   return matrix(K, xx.nrows(), xx.ncols(),
            [padic_cyclotomic_reconstruction(K, w, p, prec, phi)
for w in xx.list()])
```

```
K.<z> = CyclotomicField(3)
A = matrix(K, 2, [1+z, z, 1/2, 3*z])
v = matrix(K, 2, 1, [1-z, 2])
```

```
A \ v
```

```
    [-42/31*z - 38/31]
    [-27/31*z - 20/31]
```

```
solve_cyclo(A, v, 20)
```

```
    p =  1033
    20
    Time: CPU 0.00 s, Wall: 0.00 s
    [-42/31*z - 38/31]
    [-27/31*z - 20/31]
```

```
K.<z> = CyclotomicField(4)
n = 100
A = matrix(K, n, [K(ZZ['x'].random_element()) for _ in
xrange(n^2)])
v = matrix(K, n, 1, [K(ZZ['x'].random_element()) for _ in
xrange(n)])
```

```
time B,w = solve_cyclo(A, v, 30, 389)
```

```
    p =  389
    CPU time: 1.99 s,  Wall time: 2.08 s
```

```
C = B.change_ring(GF(389))
time k = C.echelon_form()
```

```
    Time: CPU 0.00 s, Wall: 0.00 s
```

```
time w = A\v
```

```
    CPU time: 0.00 s,  Wall time: 0.00 s
```

```
show(A)
```

$$\left(\begin{array}{rrrrr}
z + 2 & -8z + 1 & z - 4 & -z - 73 & -z - 7 \\
-4 & 26 & z + 1 & -z - 1 & 24 \\
z - 1 & -3z - 4 & 1 & -z + 6 & -2z - 5 \\
-z + 10 & -3 & 9 & z - 5 & -z + 3 \\
-5z - 1 & z - 9 & z - 2 & -10 & -z + 3
\end{array}\right)$$

```
(A \ v)[0]
```

```
    (-6729862772043/126283901266*z - 1244663322069/63141950633)
```

```
time solve_cyclo(A, v, 40, 2^15)[0]
```

```
    p =  32789
    20
    Time: CPU 0.04 s, Wall: 0.04 s
```

```
(-6729862772043/126283901266*z - 1244663322069/63141950633)
CPU time: 0.07 s,  Wall time: 0.07 s
```