

MODSR: Modular solve and roots

Herbert Melenk

Konrad-Zuse-Zentrum für Informationstechnik Berlin

Takustraße 7

D-14195 Berlin-Dahlem, Germany

e-mail: melenk@zib.de

March 20, 2004

This package supports the SOLVE and ROOTS operators for modular polynomials and modular polynomial systems. The moduli need not be primes. M_SOLVE requires a modulus to be set. M_ROOTS takes the modulus as a second argument. For example:

```
on modular; setmod 8;
m_solve(2x=4);           ->  {{X=2},{X=6}}
m_solve({x^2-y^3=3});
  ->  {{X=0,Y=5}, {X=2,Y=1}, {X=4,Y=5}, {X=6,Y=1}}
m_solve({x=2,x^2-y^3=3}); ->  {{X=2,Y=1}}
off modular;
m_roots(x^2-1,8);       ->  {1,3,5,7}
m_roots(x^3-x,7);      ->  {0,1,6}
```