16.40 MODSR: Modular solve and roots

This package supports solve (M_SOLVE) and roots (M_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}
```

The operator `legendre_symbol`(a,p) denotes the Legendre symbol

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

which, by its very definition can only have one of the values $\{-1, 0, 1\}$.

There is no further documentation for this package.

Author: Herbert Melenk.