Paradigms of PARI programming

Karim Belabas

http://pari.math.u-bordeaux.fr/

UNIVERSITÉ PARIS-SUD 11

Warning

This talk focuses on the current development version of the PARI library (2-2-8, to be released), freely available from anonymous CVS (Concurrent Version System), see

`http://pari.math.u-bordeaux.fr/CVS.html`

Lucas's test for Mersenne primes

Let p be a prime number and $q := 2^p - 1$. Let

$$u_2 = 4; \quad u_{i+1} = u_i^2 - 2 \pmod{p} \quad \text{for } i > 2.$$

Then q is prime iff $u_p = 0$.

Berlekamps primality test over $\mathbb{F}_p[X]$

Let p a prime number, $A \in \mathbb{F}_p[X]$ a squarefree polynomial. Let Q the endomorphism $\mathrm{Frob}_p - \mathrm{Id}$ of the *etale* algebra $\mathbb{F}_p[X]/(p, A)$. Then $\dim_{\mathbb{F}_p} \mathrm{Ker}\, Q = \omega(A)$, the number of distinct irreducible factors of A.

Extended Euclidean algorithm

Let x, y two integers and initially $\left(\begin{smallmatrix} s_x & s_y \\ t_x & t_y \end{smallmatrix}\right) = \mathrm{Id}$,

$$\begin{pmatrix} s_x & s_y \\ t_x & t_y \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

To apply ordinary Euclidean algorithm to right hand side, multiply the system from the left by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & -q \end{smallmatrix}\right)$, with $q = \lfloor x/y \rfloor$. Iterate until $y = 0$ then the first line of the system reads

$$s_x x + s_y y = \gcd(x, y).$$

In practice, there's no need to update s_y and t_y since $\gcd(x, y)$ and s_x are enough to recover s_y.

Modular Determinant for $A \in M_n(\mathbb{Z})$

Compute $\det A$ modulo several single precision primes p_i. Then use Chinese remainders to compute $\det A$.

Rigorous if $\prod_i p_i > 2\,|\det A|$. The determinant is bounded by $\prod_j \|A_j\|_2$ for instance.