FAST JACOBIAN ARITHMETIC ON $C_{3,4}$ CURVES

KAMAL KHURI-MAKDISI (WITH F. ABU SALEM)

This talk is based on the paper math.NT/0610121, which will appear in the LMS J. Comp. Math.

Let k be a very large finite field. A $C_{3,4}$ curve over k is a curve C with a distinguished k-point P_∞ such that the affine curve $U := C - P_\infty$ has affine coordinate ring of the form $R = k[x,y]/(y^3 + p_2(x)y = x^4 + q_2(x))$ with $v_\infty(x) = -3$ and $v_\infty(y) = -4$, where $\deg p_2 \leq 2$ and $\deg q_2 \leq 2$. The genus of C is 3. These form a 5-dimensional family of the 6-dimensional moduli space.

We want explicit (efficient) formulas for adding 2 points in k. Restricting to $C_{3,4}$ curves makes it easier to write down the equations.

Recall that $|k|$ is very large. Therefore we will give operation counts only for adding two "general" elements of $J(k)$. We count only multiplications and inversions: the reason for this is that these operations are significantly slower than addition for large fields. "General" means that the probability of an element being non-general should be $O(1/|k|)$; hence they should never be seen in practice. If we come across them, there exist general algorithms for curves of any genus (KKM, Math. Comp., soon, and arXiv 0409209).

The following table gives the number of multiplications and inversions required for adding or doubling general elements of $J(k)$, in our work, and in work of two earlier groups of researchers:

	Basiri Enge Faugère Gürel	Flon Oyono Ritzenthaler	Abu Salem KKM
addition	150M, 2I	145M, 2I	117M, 2I
doubling	174M, 2I	167M, 2I	129M, 2I

The earlier groups represented an effective divisor on D on C by an ideal I_D of R: they use an analogue of the Mumford representation, namely $I_D = \langle f(x), y - g(x)\rangle$ where $\deg f = d$ and $\deg g = d - 1$.

We try to be as economical as possible with respect to v_∞.

Let $w^N := H^0(C, N \cdot P_\infty) = \{f \in R : v_\infty(f) \geq -N\}$. If D is an effective divisor of degree d not containing P_∞, then $w^N_D := H^0(C, N \cdot P_\infty - D) = I_D \cap w^N$. For $N \geq 5$, we have $\dim w^N = N - 2$. For $N - d \geq 3$ and D general, we have $\dim w^N_D = N - d - 2$.

Overview of algorithms: Represent a general element of $J(k)$ as $[D - 3P_\infty]$ where D is effective of degree 3. Generally, w^7_D is 2-dimensional and has basis $F := x^2 + ay + bx + c$, $G := xy + dy + ex + f$. Represent $[D - 3P_\infty]$ or I_D by the pair $\{F, G\}$: store $\{a, b, \ldots, f, a^{-1}\}$, where a^{-1} is there for technical convenience. Fact: $I_D = \langle F, G\rangle$. Caution: $\{F, G\}$ is not a Gröbner basis.

Date: July 23, 2007.

Strategy for Jacobian addition. D, D' are general, so $D \cap D' = \emptyset$. Represent D and D' by $\{F, G\}$ and $\{F', G'\}$.

(1) Find $0 \neq s \in w^9_{D+D'}$ so that $I_{D+D'} = \langle s, t\rangle$. We also need $t \in w^{10}_{D+D'}$.

$$(s) = D + D' + D'' - 9P_\infty$$

where $\deg D'' = 3$. The set $\{s, t\}$ is a basis for $w^{10}_{D+D'} = w^{10}_D \cap w^{10}_{D'} \subset w^{10}$, and the last space is 8-dimensional. Each space in the intersection is 5-dimensional: e.g., the first has basis F, G, xF, yF, xG.

(2) We want to find $w^7_{D''}$. Note:

$$I_{D''} = (I_{D+D'+D''} : I_{D+D'}) = (\langle s\rangle : \langle s, t\rangle) = \{f \in R : ft \in \langle s\rangle\}.$$

Take intersection with w^7:

$$w^7_{D''} = \{f \in w^7 : ft \in sw^8\}.$$

This amounts to finding $tw^7 \cap sw^8$. It looks like an intersection of a 5-dimensional space and a 6-dimensional space in w^{17}, which is 15-dimensional, but the intersection takes place in $w^{17}_{D+D'}$, which is 9-dimensional, so we get a 2-dimensional intersection.

(3) The final inversion is not hard: it takes 7M, included in the above count.

Remark 0.1. If one is interested only in taking high powers of an element, one can delay the final inversions until the very end: this speeds up things a little.