

XMINV	1	pose $[A2] \equiv [A0]^{-1} \pmod{[A1]}$
XMINVS _{1/4}	3	" $[A2] \equiv [A0]^{-1} \pmod{[A1]}$
XMPOSE	4	" $[A2] = [A0] \pmod{[A3]}$
XMCHG	5	change le signe de $[A2] \pmod{[A3]}$
XMMUL	6	pose $[A2] = [A0] * [A1] \pmod{[A3]}$ $[A0] \text{ et } [A1] \geq 0$
XMMULS	6a	" " " 99
XMADD	7	" $[A0] + [A1]$ " $[A0], [A1] \in [0, p[$
XMSUB	8	" - "
XMEXP	9	" $= [A0]^{[A1]}$
XRND	12	" $= \text{rnd}([A0])$
XRNRG	12a	pose do.L = rnd(D1.L)
XMPT _{1/2}	13	teste si $[A0]$ est premier EQ ₉₉ probablement $\begin{cases} 1 \text{ pair ou impair} \\ 2 \text{ impair} \end{cases}$
XMPT	16	teste si $[A0]$ est premier met $[A2] = \begin{cases} -1 & \text{oui (probablement)} \\ 0 & \text{non} \end{cases}$
XMPRS1	18	} $\text{met premier}([A0]) = \text{nb premier } \geq [A0]$ $> [A0]$
XMPRS2	19	
XMPRS _A	19a	
XMPRS	20	
XMPSB	21	pose $[A2] \equiv [A0] \pmod{[A3]}$ balanced

XMPRND	21a	pose $P_{A_2} = \text{rnd}([A_3], \overset{D_0}{x}, \overset{D_1}{k})$
XMPNOR	22	pose $P_{A_2} \equiv \lambda P_{A_0} \pmod{[A_3]}$ normaliser
XMPCMUL	23	pose $P_{A_2} \equiv [A_1] * P_{A_0} \pmod{[A_3]}$ (cas $P_{A_0} [A_1] \geq 0$)
XMPCMUL ^T	23a	" " (" [A1] < 0)
XMP PB	24	pose $P_{A_2} \equiv P_{A_0} \pmod{[A_3]}$ coef $\in [-\frac{p}{2}, \frac{p}{2}[$ balanced
XMP PM	25	" $P_{A_2} \equiv P_{A_0}$ " coef $\in [0, p[$
XMP TR	26	traite $P_{A_0} \rightarrow P_{A_2}$ suivant (P) 14 agissant sur $[A_0]$
XMP ADD	27	pose $P_{A_2} \equiv P_{A_0} + P_{A_1} \pmod{[A_3]}$
XMP SUB	28	" - "
XMP MUL	29	" * "
XMP MOD ^H	31	" $\equiv P_{A_0} \pmod{[A_3]}$ et $\pmod{v(x)}$ où $v(x) = \frac{P_{A_4}}{P_{A_1}}$
XMP DIV	32	pose $\begin{matrix} A^3 & A^2 \\ \hline \square & \square \end{matrix}$ (division de P_{A_0} par $P_{A_1} \pmod{[A_3]}$)
XMM MUL	33	pose $P_{A_2} = P_{A_0} * P_{A_1} \pmod{[A_3]}$ et $\pmod{P_{A_4}}$
XMPEXP	34	pose $P_{A_2} = P_{A_0}^{[A_1]} \pmod{[A_1]}$ et $\pmod{P_{A_4}}$
XMP DEG	36	$DS = \text{deg } P_{A_0}$ (unitaire)
XMP GCD ¹	37	pose $P_{A_2} \equiv \text{pgcd}(P_{A_0}, P_{A_4}) \pmod{[A_3]}$
XMP INV	38	" $\equiv (P_{A_0})^{-1} \pmod{[A_3]}$, $\pmod{P_{A_4}}$
XMP SQF	41	déterminer si P_{A_0} est sans facteurs multiples $\pmod{[A_3]}$
XMF MD ₁	42	factorise Φ produit de fact irréductibles de degré d mod p
XF REP	43	remplace un facteur dans expression factorisée
XMF PAR	47	(SP) de XMF MD ₁
XMF PLU ^Q	48	pose $\text{var}_{A_2} =$ forme factorisée de $P_{A_0} \pmod{[A_3]}$ { cas facteurs multiples ou non
XMF BEZ	50	Calcule v_i : $\frac{v_1}{u_1} + \frac{v_2}{u_2} + \dots + \frac{v_k}{u_k} \equiv \frac{1}{u_1 \dots u_k} \pmod{[A_3]}$
XMF BEZC	55	vérif que var_{A_0} est produit de poly $u_i(x)$ (in littéral)
XMF INT	56	pose $\text{var}_{A_2} =$ forme factorisée de P_{A_0} sans facteurs multiples $\in \mathbb{Z}[x]$
XF REP ₁	67a	Modifie les facteurs de var_{A_1} suivant SP(A ₂) (SP) de XMF INT
LIFTB	68] (SP) de XMF INT
LIFTA	69	
XPP	70	
		pose $\text{pp}(f(x))$ $f(x) \in \mathbb{Z}[x]$

XJPDIV	80	<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px; margin-right: 5px;"> $\begin{matrix} A^3 & A^2 \\ R & Q \end{matrix}$ </div> <div style="margin-left: 10px;"> $: P_{A0} = P_{A1} * Q + R$ dans $Q[x]$ </div> </div>
XJPMOD	82	pose $P_{A2} \equiv P_{A0} \text{ mod } P_{A1}$ dans $Q[x]$
XJPINV	83	<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px; margin-right: 5px;"> $\begin{matrix} A^2 & A^3 & A^6 \\ a & P & \end{matrix}$ </div> <div style="margin-left: 10px;"> $P = \text{pgcd}(P_{A0}, P_{A1})$ normalisé } dans $Q[x]$ $aP_{A0} + bP_{A1} = P$ </div> </div> <p>[Euclide étendu]</p>
XJPDHG	86	pose $P_{A2} = \text{dehomog}(P_{A0}, z)$ ($z = P_0$)
XJPSCT	87	pose $P_{A2} = \text{subs}(P_{A0}, z = D.L)$
XJPANY	88	pose en A_2 la table des exposants de P_{A0}
XJPHTS	89	teste si P_{A0} est homogène oui \Leftrightarrow EQ vrai comme A_0
XJPHMG	90	pose $P_{A2} = \text{homog}(P_{A0}, z)$
XJPHMG1	92	var_{A2} "
XJFHMG	93	var_{A2} " (var_{A0}, z)
XFREC	94	réécrit var_{A0} en transformant chaque facteur par le SP (A_1) [paramètre D_0]
CALPRO	94a	calcule un produit
XJFG	95	pose $\text{var}_{A2} = \text{formf}(P_{A0})$ où P_{A0} sans facteur multiples, ni linéaires
XJFF	97	pose A et B facteurs de P_{A0} si possible
ANALDG	114	sp de XJFF
XJPSAB	117	remplace P_{A0} (entiers) par $\text{subs}(P_{A0}, y = y + ax + b)$
SUALT	118	$D_3 = \begin{cases} 1 - D_1 \\ -D_1 \end{cases}$

factorisation
de
polynôme
à plusieurs
littéraux

- XFRL1 120 entrée P_{A_0} , DO sortie $var_{A_2} = P_{A_0}$ factorisé suit $cont_x$ $x \geq DO$
- XREDQL (283a) remplace var_{A_0} par plus factorisé suivant $cont_x$
- XGQU 123 entrée P_{A_0}, P_{A_1} sortie $d = \text{pgcd}(P_{A_0}, P_{A_1})$, $a = P_{A_0}/d$ et $b = P_{A_1}/d$
- XFRM2 123a entrée P_{A_0} factorise les facteurs multiples
1 " (et x) " "
- XREDQM (283b) remplace var_{A_0} par factorisé de "