MWM	IAC bir IAC RA y start	nary fie	eld poi	nt add	ition f	unctio	n Mem	nory p	lan			B8		B7		36	B5		34	В:	2	B2		B1
23 22	2 21 20	X4 X3  19 18	17 16					A8 A7	A6 A5	A4 A3	A2 A1 1 1 0	TS8	7 15 23 31	P7 1. TS7 2 TC7 3	T T	5 26 13 S6 21 C6 29	TS5	12 7 20	3P4 11 TS4 19 TC4 27	TC	10 3 18	TS2	1 9 17 25	TS1 16
<b>X</b>	<b>Y</b> / X6 X5	<b>Z</b>	<b>X</b> X2 X1	<b>Y</b> E8 E7	<b>Z</b> E6 E5	<b>A</b> E4 E3	<b>B</b>	<b>R2</b> A8 A7	<b>R</b> A6 A5	A4 A3	A2 A1	B8 P8 TS8	B 7 n(x) 15	B7 (P7 1	6 .4 T	A 36 5 n(x) 13	P5 TS5	12 T	P4 11 	Y B3	2 3 10 3	B2 P2 TS2	X 1 n(x) 9	B1 0 P1 8
01 =	Z1*Z1*	rinvpolyult(E5, E	у			СоруН			5 4	3 2 <b>01</b>	1 0	TC8 B8	23 31 B 7 n(x)	2 TC7 3	6 E	21 C6 29 A 36 5 n(x)	TC5 B5	4	P4	Y B3	3 2	TC2 B2 P2	25 O1 1 n(x)	TC1 24
O2 =	2 21 20 Z2*Z2*	x4 x3  19 18  Frinvpolult(X3,X)	17 16 y		13 12	11 10 CopyH	9 8	7 6 B7)	A6 A5	3 2 O1	1 0	TS8 TC8	23 31	TS7	T T	13 S6 21 C6 29	TS5	20 7 28	11 754 19 7C4 27	TS	18 3 26	TS2 TC2	9 17 25	TS1 16 TC1 24
$\begin{array}{ccc} X8 & X7 \\ \hline 23 & 22 \\ A = X \end{array}$	x6 x5	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7	A6 A5	A4 A3 3 2		P8 TS8 TC8	7 n(x) 15 23 31	P7 1. TS7 2	6 .4 T	5 n(x) 26 13 56 21 C6 29	P5	12 7 20	3	TS	2 3 10 3	P2 TS2 TC2	1 n(x) 9 17 25	TS1 16
<b>X2</b> X8 X7	<b>Y2</b> 7 X6 X5	<b>Z2</b>	<b>X1</b> X2 X1		<b>Z1</b> E6 E5	<b>A(P)</b> E4 E3	<b>B(P)</b> E2 E1	R2	<b>R</b> A6 A5	<b>O1</b> A4 A3		P8 TS8 TC8	7 n(x) 15 23	P7 1. TS7 2 TC7 3	6 F	66 5 n(x) 66 13 66 21 66 29	TS5	12 7	3 n(P4 11 154 19 154 19 154 154 154 154 154 154 154 154 154 154	TS	2 3 10 3	B2 P2 TS2 TC2	1 n(x) 9 17	B1 C P1 8 TS1 16 TC1 24
B3 =	Y2	invpoly ult(X7,A	X1	<b>Y1</b> E8 E7	<b>Z1</b>		B(P)	R2	<b>R</b> A6 A5	<b>O1</b> A4 A3	A2 A1	B8 P8 TS8	02 7 n(x) 15	B7 (P7 1.TS7 2	6 .4 T	A 5 n(x) 6 13 56 21	P5 TS5	12	<sup>B4</sup> 3	B B3 ( <b>x</b> ) P3	3 10	B2 P2 TS2	B 1 n(x) 9	B1 C P1 8 TS1 16
T1 = 1 B7 =	Y1*O2* MontMu	rinvpolyult(E7,B	7,P1)	Y1	<b>Z1</b>	СоруН: <b>А(Р)</b>	2H(B1, <b>B(P)</b>	R2	5 4	<b>01</b>	1 0	TC8  B8	31 T1 7 n(x) 15	TC7 3	6 E	29 29 36 5 n(x)	B5 P5	4	<sup>B4</sup> 3	B B3	26	TC2 B2 P2	25 T1 1 n(x) 9	TC1 24
23 22 C = T	21 20 1*Z2*ri	19 18	17 16		13 12		9 8	7 6	5 4	3 2		TS8	31	TS7 2 TC7 3	7.2 T	21 C6 29	TC5	20	TS4 19	TC	18	TS2	<u>17</u> <u>25</u>	TS1 16
T2 = 1	Y2*O1*	<b>Z2</b> X4 X3  19 18  rinvpolyult(X5,A	17 16		13 12		9 8	7 6	<b>R</b> A6 A5	<b>O1</b> A4 A3		P8 TS8 TC8	7 n(x) 15 23	P7 1. TS7 2 TC7 3	6 F	66 5 n(x) 66 13 66 21 66 29	TS5	12 7 20	<sup>B4</sup> 3	TS	3 18	P2 TS2 TC2	1 n(x) 9 17	P1 8 TS1 16 TC1 24
23 22 D = T	2 21 20 2*Z1*ri	<b>Z2</b> X4 X3  19 18  invpoly ult(A3,E	17 16		13 12	E4 E3	9 8	7 6	<b>R</b> A6 A5	<b>T2</b> A4 A3	A2 A1 ·	P8 TS8 TC8	7 n(x) 15 23	P7 1. TS7 2 TC7 3	6 .4 T	5 n(x) n(x) 13 S6 21 C6 29	TS5	12 7	B4 3	TS	3 18	P2 TS2 TC2	1 n(x) 9 17 25	B1 C P1 8 TS1 16 TC1 24
		<b>Z2</b> X4 X3				E4 E3		<b>R2</b> A8 A7	<b>R</b> A6 A5	<b>D</b> A4 A3	A2 A1 1 0	P8 TS8 TC8	7 n(x) 15 23	TC7	6 .4 T	A 5 n(x) 13 S6 21 C6 29	TS5	12 20	<sup>84</sup> 3	TC	3 18	B2 P2 TS2 TC2	D 1 n(x) 9 17	B1 C P1 8 TS1 16 TC1 24
Х2	Y2	<b>Z2</b>	X1	<b>Y1</b> E8 E7	Z1		B(P)	R2	<b>R</b> A6 A5	<b>D</b>	A2 A1	B8 P8 TS8	F 7 n(x) 15		6 .4 T	A 5 n(x) 13 S6 21	TS5	12 20	3 n( P4 11 TS4 19		3 18	B2 P2 TS2	F 1 n(x) 9	B1 C P1 E TS1 TC1
E = A A3 =	+B ModAdd	19 18 d(B5,B3	s,P1)	Y1	<b>Z1</b>	СоруН: <b>А(Р)</b>	2H(B1,	R2	<b>R</b> A6 A5	<b>D</b>	1 0	B8 P8 TS8	31 F 7 n(x) 15	B7 (P7 1:	6 F	E 5 n(x) 13 S6	B5 P5	4 12	3 <b>n</b> ( P4 11	B B3	26 3 10	B2 P2 TS2	25 E 1 n(x)	TC1 24  B1 C  P1 8  TS1 16
G = E	*Z1*rin	19 18 avpoly ult(B5,E		15 14 <b>Y1</b>		СоруН		7 6 B3)	5 4	3 2 <b>D</b>	1 0	TS8 TC8 B8	23 31 <b>F</b> 7 <b>n(x)</b>	2 TC7 3	T T	21 C6 29 E 36 5 n(x)	TC5	20 7 28	19 CC4 27	TC	18 3 26	TS2 TC2 B2	17 25 <b>G</b> 1 n(x)	TS1 16 TC1 24  B1 C
23 22 T3 =	21 20 F*X2*ri	19 18	17 16		13 12	11 10	9 8	7 6	A6 A5	3 2 <b>T3</b>	A2 A1 ·	TS8 TC8	15 23 31	TS7	T T T T T T T T T T T T T T T T T T T	26 13 S6 21 C6 29 E	TS5	12 20 T 28	754 19 7C4 27	TS TC	10 3 18 3 26	TS2 TC2	9 17 25	P1 8 TS1 16 TC1 24
23 22 T4 =	x6 x5 2 21 20 G*Y2*ri	X4 X3	X2 X1	E8 E7	E6 E5	E4 E3	E2 E1	A8 A7		<b>T3</b> A4 A3	A2 A1 ·	P8 TS8 TC8	7 n(x) 15 23	P7 1. TS7 2 TC7 3	6 .4 T	5 n(x) n(x) 13 S6 21 C6 29	P5	12 20	3	TS	3 18	P2 TS2 TC2	1 n(x) 9 17	TS1 16
23 22	2 21 20	<b>Z2</b> X4 X3				E4 E3		<b>R2</b> A8 A7	<b>T4</b> A6 A5	<b>T3</b> A4 A3	A2 A1 ·	P8 TS8 TC8	7 n(x) 15 23 31	B7 (P7 1 1 TS7 2 TC7 3	6 F	E  5  n(x)  13  S6  21  C6  29	TS5	12 20	B4 3	TS	3 18	B2 P2 TS2 TC2	1 n(x) 9 17	B1 C E E E E E E E E E E E E E E E E E E
<b>X2</b> X8 X7	<b>Y2</b> X6 X5	<b>Z2</b> X4 X3	<b>X1</b> X2 X1		<b>Z1</b> E6 E5	E4 E3	<b>B(P)</b> E2 E1	R2	<b>T4</b> A6 A5	<b>H</b> A4 A3	A2 A1	B8 P8 TS8 TC8	7 n(x) 15 23	B7 (P7 1. TS7 2 TC7 2.	6 .4 T	E  5  6  13  56  21	TS5	12 T 20	3 n(P4 11 154 19 154 19 154 154 154 154 154 154 154 154 154 154	TS	3 18	B2 P2 TS2 TC2	H 1 n(x) 9	B1 C
Z3 = X3 =	G*Z2*ri MontMu	invpoly ult(B3,X	(3,P1)	Y1	Z1	СоруН: <b>А(Р)</b>	2V(B1,)	R2	<b>T4</b> A6 A5	<b>H</b>	A2 A1	B8 P8 TS8	7 n(x) 15	B7 (P7 1:	6 .4	29  E 5 n(x) 13 S6 21	B5 P5	12	B4 3	<b>G</b> B3	3 10	B2 P2 TS2	25 23 1 n(x) 9	B1 0 P1 E
I = F- A5 =	-Z3 ModAdd	19 18 d(B7,X3	x1	Y1	<b>Z1</b>	СоруН: <b>А(Р)</b>	2V(B1,,	R2	5 4	<b>H</b>	1 0	TC8  B8  P8	31 F 7 n(x)	TC7 3	6 E	E 5 n(x)	B5	4	B4 3	TC B3	26	TC2 B2 P2	25 I n(x)	TC1 24
23 22 T5 = 1	2 21 20 Z3*Z3*	rinvpolyult(X3,X	17 16		13 12	11 10	9 8	7 6	5 4		1 0	TS8 TC8	23 31 <b>F</b> 7 <b>n(x)</b>	TS7 2 TC7 3	T T	21 C6 29 E 36 5 n(x)	TC5	20 7 28	B4 3	TC	18 3 26	TS2 TC2 B2	17 25 <b>T5</b> 1 n(x)	TS1 16 TC1 24
23 22 T6 =	21 20 apoly_n	X4 X3 19 18 mont*T5 ult(E3,A	17 16 5*rinvpo	15 14	13 12		9 8	7 6	A6 A5	A4 A3	A2 A1	TS8	15 23 31	P7 1. TS7 2 TC7 3	T T	26 13 S6 21 C6 29	TS5	12 7 20	P4 11 154 19 19 19 19 19 19 19 19 19 19 19 19 19	TS	10 3 18	TS2	9 17 25	P1 8 TS1 16 TC1 24
23 22 T7 =	2 21 20 F*I*rinv	19 18	17 16		13 12	E4 E3	9 8	A8 A7	A6 A5	<b>H</b> A4 A3	A2 A1	P8 TS8 TC8	7 n(x) 15 23	P7 1. TS7 2 TC7 3	6 F	66 5 n(x) 66 13 56 21 56 29	TS5	12 20	B4 3	B3 P3 TS	3 18	P2 TS2 TC2	1 n(x) 9 17	B1 C
<b>X2</b> X8 X7	<b>Y2</b> X6 X5	<b>Z3</b> X4 X3	<b>X1</b> X2 X1		<b>Z1</b> E6 E5		<b>B(P)</b> E2 E1	Т6	A6 A5	<b>H</b> A4 A3	A2 A1	P8 TS8 TC8	7 n(x) 15 23	P7 1 TS7 2 TC7 3	6 F	E 5 7 86 13 86 21	TS5	12 20	<sub>84</sub> 3	TC	3 18	P2 TS2 TC2	1 n(x) 9 17 25	B1 C P1 8 TS1 16 TC1 24
X2  X8 X7	<b>Y2</b> X6 X5	<b>Z3</b> X4 X3	<b>X1</b> X2 X1		<b>Z1</b> E6 E5	E4 E3	<b>B(P)</b> E2 E1	Т8	<b>I</b> A6 A5	<b>H</b> A4 A3	A2 A1 1	B8 P8 TS8 TC8	7 7 n(x) 15 23	B7 (P7 1: TS7 2 TC7 3	6 F	E  5  n(x)  13  56  21	TS5	12 20	B4 3	TS	3 18	B2 P2 TS2 TC2	T8 1 n(x) 9 17	B1 C P1 8 TS1 16 TC1 24
B7 =	Y2	z3	X1	<b>Y1</b> E8 E7	Z1	<b>A(P)</b>	B(P)	Т8	<b>I</b> A6 A5	<b>H</b> A4 A3	A2 A1	B8 P8 TS8	T9 7 n(x) 15	B7 P7 1. TS7 2	6 .4 T	E 5 n(x) 6 13 S6 21	P5 TS5	12	B4 3	TS	3 10	B2 P2 TS2	T9 1 n(x) 9	B1 C P1 8 TS1 16
T10 =	: T9*E*ı	rinvpolyult(B7,B	,	15 14 <b>Y1</b>		СоруН		7 6 B7)	5 4	3 2 H	1 0	TC8	7 n(x)	TC7 3	6 E	C6 29 E 6 5 n(x)	TC5	28	CC4 27	TC	3 26	TC2 B2 P2	25 T10 1 n(x)	TC1 24
23 22 X3 =	2 21 20 T8+T10	19 18	17 16		13 12		9 8	7 6	A6 A5	A4 A3 3 2	A2 A1 ·	TS8	15 23 31	TS7 2 TC7 3	T 22	13 S6 21 C6 29	TS5	12 7 20	11 54 19 5C4 27	TS	10 3 18	TS2 TC2	9 17 25	TS1 16
23 22 T11 =	21 20 : I*X3*r	19 18	17 16			E4 E3		<b>T8</b> A8 A7	A6 A5	<b>H</b> A4 A3	A2 A1	P8 TS8 TC8	7 n(x) 15 23	P7 1. TS7 2 TC7 3	6 .4 T	5 n(x) 6 13 56 21 66 29	TS5	12 7 20	B4 3	TC	3 18	P2 TS2 TC2	1 n(x) 9 17 25	B1 C
<b>X3</b> X8 X7	<b>Y2</b> / X6 X5	<b>Z3</b> X4 X3	<b>X1</b> X2 X1		<b>Z1</b> E6 E5	E4 E3	<b>B(P)</b> E2 E1	T11	<b>A</b> 6 A5	<b>H</b> A4 A3	A2 A1 ·	B8 P8 TS8 TC8	7 n(x) 15 23	B7 P7 1. TS7 2 TC7 3	6 4 T	E 5 n(x) 13 S6 21 C6 29	TS5	12 20	B4 3	тс	3 18	B2 P2 TS2 TC2	T11 1 n(x) 9 17	B1 0 8 TS1 16 TC1 24
T12 = B7 =	· G*G*ri MontMu <b>Y2</b>	invpoly ult(B3,B	3,P1)	Y1	<b>Z1</b>	СоруН: <b>А(Р)</b>	2H(B1,	T11	<b>I</b> A6 A5	<b>H</b>		B8 P8 TS8	7 n(x)	B7 P7 1. TS7	6 F	E 36 5 n(x)	B5 P5	12	34 3 n( P4 11	<b>G</b> B3 ( <b>x</b> ) P3	3 2	B2 P2 TS2	T12 1 n(x) 9	B1 C P1 8
T13 =	: T12*H	19 18 *rinvpo ult(B7,A	ly	15 14 <b>Y1</b>		11 10 CopyH:			5 4	3 2 <b>H</b>	1 0	TC8	23 31 <b>T13</b> 7 n(x)	7C7	T T	21 C6 29	TC5	20 T 28	19 CC4 27	TC	18 3 26	TC2	17 25 <b>T13</b> 1 n(x)	TC1 24
23 22 Y3 = 1	21 20 T11+T1	19 18	17 16		13 12	11 10	9 8	7 6	A6 A5	A4 A3	A2 A1 ·	TS8	15 23 31	P7 1. TS7 2 TC7 3	T	13 S6 21 C6 29	TS5	12 7 20	P4 11 15 15 15 15 15 15 15 15 15 15 15 15	TS	3 18	TS2	9 17 25	P1 8 TS1 16 TC1 24
X5 = X3	<b>Y3</b>	<b>Z3</b>	<b>X1</b> X2 X1		<b>Z1</b> E6 E5	E4 E3	<b>B(P)</b> E2 E1	T11	A6 A5	<b>H</b> A4 A3	A2 A1	P8 TS8 TC8	7 n(x) 15 23	TS7 2	6 .4 T	E  36  5  n(x)  13  S6  21  C6  29	TS5	12 20	34 3	TS	3 18	P2 TS2 TC2	<b>Y3</b> 1  n(x)  9  17	B1 C C E E E E E E E E E E E E E E E E E
O1 = A3 = Copyl O2 = B7 =	MontMu H2V(B1 Z2*Z2*	rinvpoljult(E5, E , A3) rinvpoljult(X3,X	E5, P1) y																					
B5 = Copyl  B = X  B3 = Copyl  T1 = B7 =	MontMu H2H(B1 2*O1*ri MontMu H2H(B1 Y1*O2*	invpoly ult(X7,A ,B3) rinvpoly ult(E7,B	37,P1) .3,P1)																					
B7 = Copyl T2 = A3 = Copyl D = T A3 =	MontMi H2H(B1 Y2*O1* MontMi H2V(B1 '2*Z1*ri	rinvpoly ult(X5,A , A3) invpoly ult(A3,E	(3,P1) / (3,P1)																					
Copyl E = A A3 = Copyl G = E B3 =	ModAdd H2H(B1 +B ModAdd H2H(B1 *Z1*rin	d(B5,B3 ,B5) ivpoly ult(B5,E	s,P1)																					
A3 = Copyl T4 = A5 = Copyl H = T A3 =	H2V(B1 G*Y2*ri MontMu H2V(B1 G3+T4	ult(B7,X ,A3) nvpoly ult(B3,X ,A5)	(5,P1)																					
Z3 = X3 = Copyl I = F+ A5 = Copyl T5 = A7 =	G*Z2*ri MontMu H2V(B1 -Z3 ModAdd H2V(B1 Z3*Z3*	invpoly ult(B3,X ,X3) d(B7,X3 ,A5) rinvpoly ult(X3,X	(3,P1) (1)																					
T6 = A7 = Copyl  T7 = B7 = Copyl  T8 = A7 =	apoly_n MontMu H2V(B1 F*I*rinv MontMu H2H(B1 T6+T7	nont*T5 ult(E3,A ,A7) poly ult(B7,A ,B7)	7,P1) .5,P1)	oly																				
T9 = B7 = Copyl  T10 = B7 = Copyl  X3 = X7 =	E*E*ring MontMu H2H(B1 F T9*E*I MontMu H2H(B1 ModAdd	vpoly ult(B5,B ,B7) rinvpoly ult(B7,B ,B7) ) d(A7,B7	, 5,P1)																					
Copyl T11 = A7 = Copyl T12 = B7 = Copyl	H2V(B1 I*X3*r MontMu H2V(B1 G*G*r MontMu H2H(B1	,X7) invpoly ult(A5,X ,A7) invpoly ult(B3,B	(7,P1) (3,P1)																					
B7 = Copyl Y3 = X5 =	MontMı H2H(B1 T11+T1	ult(B7,A ,B7) L3 d(A7,B7	.3,P1)																					