

Лабораторная работа №1

«Проверка чисел на простоту»

Задание. Написать программу, реализующую тест Миллера – Рабина проверки на простоту следующих чисел для любого целого числа a . Если число проходит тест, то выбрать другое случайное число a и повторить тест. Достаточно повторить тест Миллера – Рабина пять раз. Выводить все промежуточные результаты.

Вариант	
1	99601; 99607
2	99611; 99613
3	99623; 99629
4	99643; 99647
5	99653; 99661
6	99667; 99677
7	99679; 99683
8	99689; 99691
9	99703; 99707
10	99721; 99727
11	99733; 99751
12	99761; 99763
13	99767; 99779
14	99787; 99791
15	99793; 99797
16	99811; 99817
17	99821; 99823
18	99821; 99829
19	99833; 99839
20	99857; 99859
21	99871; 99877
22	99881; 99887
23	99893; 99901
24	99907; 99919
25	99923; 99929
26	99941; 99947
27	99949; 99961
28	99971; 99973
29	99989; 99991
30	100003; 100007

Лабораторная работа №2

«Факторизация составного числа»

Задание. Найти нетривиальный делитель заданного числа ρ – методом Полларда. Для программной реализации c и f задаются пользователем. Для ручной отработки: $c = 2, f = x^2 + 1$.

Вариант	
1	5989
2	5983
3	5977
4	5969
5	5963
6	5921
7	5917
8	5893
9	5891
10	5809
11	5777
12	5771
13	5767
14	5723
15	5713
16	5699
17	5671
18	5633
19	5617
20	5611
21	5609
22	5597
23	5587
24	5561
25	5549
26	5539
27	5513
28	4897
29	4891
30	4867

Лабораторная работа №3

«Эллиптические кривые (ЭК) над полем вещественных чисел»

Задание. Реализовать программу, которая генерирует ЭК $y^2 = x^3 + ax + b$ по заданным параметрам a и b , аналитически проверяет на сингулярность, изображает заданную ЭК графически в прямоугольной декартовой системе координат. Провести анализ сингулярности ЭК по аналитическим и графическим результатам.

Лабораторная работа №4

«Сложение точек эллиптической кривой над конечным полем $GF(p)$ »

Задание. Найти все точки эллиптической кривой, заданной уравнением $y^2 = x^3 + ax + b$ над полем $GF(p)$. Выбрать две точки P и Q . Вычислить $P + Q$ и $2P$. Написать программу, реализующую алгоритм поиска всех точек эллиптической кривой, сложения и удвоения точек эллиптической кривой над конечным полем.

Вариант	a	b	p
1	1	2	17
2	1	2	19
3	1	2	23
4	1	2	29
5	1	2	31
6	2	1	17
7	2	1	19
8	2	1	23
9	2	1	29
10	2	1	31
11	2	2	17
12	2	2	19
13	2	2	23
14	2	2	29
15	2	2	31

Вариант	a	b	p
16	3	2	17
17	3	2	19
18	3	2	23
19	3	2	29
20	3	2	31
21	2	3	17
22	2	3	19
23	2	3	23
24	2	3	29
25	2	3	31
26	3	3	17
27	3	3	19
28	3	3	23
29	3	3	29
30	3	3	31

Лабораторная работа №5

«Скалярное умножение точки эллиптической кривой»

Задание. На эллиптической кривой $E_p(a; b)$, полученной в лабораторной работе №4, выбрать точку P и вычислить $7P$. Написать программу, реализующую алгоритм скалярного умножения точки эллиптической кривой $E_p(a; b)$ над конечным полем $GF(p)$.

Лабораторная работа №6

«Порядок точки эллиптической кривой»

Задание. На эллиптической кривой $E_p(a; b)$, полученной в лабораторной работе №4, выбрать точку P и определить её порядок. Написать программу, реализующую алгоритм поиска порядка точки эллиптической кривой над конечным полем.

Лабораторная работа №7

«Генерация псевдослучайных последовательностей над эллиптическими кривыми»

Задание. На эллиптической кривой $E_p(a; b)$, полученной в лабораторной работе №4, найти псевдослучайную последовательность на основе линейного конгруэнтного генератора и инверсивного генератора. Характеристики генераторов подобрать самостоятельно. Написать программу, реализующие генерацию псевдослучайных последовательностей над эллиптической кривой на основе линейного конгруэнтного генератора и инверсивного генератора.

Лабораторная работа №8

«Шифрование на эллиптических кривых»

Алфавит точек эллиптической кривой $E_{751}(1;1)$ для выполнения лабораторной работы

№	символ	точка	35	В	(67, 84)	70	е	(99, 456)	105	Й	(198, 527)
1	пробел	(33, 355)	36	С	(67, 667)	71	f	(100, 364)	106	К	(200, 30)
2	!	(33, 396)	37	D	(69, 241)	72	g	(100, 387)	107	Л	(200, 721)
3	"	(34, 74)	38	E	(69, 510)	73	h	(102, 267)	108	М	(203, 324)
4	#	(34, 677)	39	F	(70, 195)	74	i	(102, 484)	109	Н	(203, 427)
5	\$	(36, 87)	40	G	(70, 556)	75	j	(105, 369)	110	О	(205, 372)
6	%	(36, 664)	41	H	(72, 254)	76	k	(105, 382)	111	П	(205, 379)
7	&	(39, 171)	42	I	(72, 497)	77	l	(106, 24)	112	Р	(206, 106)
8	'	(39, 580)	43	J	(73, 72)	78	m	(106, 727)	113	С	(206, 645)
9	((43, 224)	44	K	(73, 679)	79	n	(108, 247)	114	Т	(209, 82)
10)	(43, 527)	45	L	(74, 170)	80	o	(108, 504)	115	У	(209, 669)
11	*	(44, 366)	46	M	(74, 581)	81	p	(109, 200)	116	Ф	(210, 31)
12	+	(44, 385)	47	N	(75, 318)	82	q	(109, 551)	117	Х	(210, 720)
13	,	(45, 31)	48	O	(75, 433)	83	r	(110, 129)	118	Ц	(215, 247)
14	-	(45, 720)	49	P	(78, 271)	84	s	(110, 622)	119	Ч	(215, 504)
15	.	(47, 349)	50	Q	(78, 480)	85	t	(114, 144)	120	Ш	(218, 150)
16	/	(47, 402)	51	R	(79, 111)	86	u	(114, 607)	121	Щ	(218, 601)
17	0	(48, 49)	52	S	(79, 640)	87	v	(115, 242)	122	Ъ	(221, 138)
18	1	(48, 702)	53	T	(80, 318)	88	w	(115, 509)	123	Ы	(221, 613)
19	2	(49, 183)	54	U	(80, 433)	89	x	(116, 92)	124	Ь	(226, 9)
20	3	(49, 568)	55	V	(82, 270)	90	y	(116, 659)	125	Э	(226, 742)
21	4	(53, 277)	56	W	(82, 481)	91	z	(120, 147)	126	Ю	(227, 299)
22	5	(53, 474)	57	X	(83, 373)	92	{	(120, 604)	127	Я	(227, 452)
23	6	(56, 332)	58	Y	(83, 378)	93		(125, 292)	128	а	(228, 271)
24	7	(56, 419)	59	Z	(85, 35)	94	}	(125, 459)	129	б	(228, 480)
25	8	(58, 139)	60	[(85, 716)	95	~	(126, 33)	130	в	(229, 151)
26	9	(58, 612)	61	\	(86, 25)	96	A	(189, 297)	131	г	(229, 600)
27	:	(59, 365)	62]	(86, 726)	97	Б	(189, 454)	132	д	(234, 164)
28	;	(59, 386)	63	^	(90, 21)	98	В	(192, 32)	133	е	(234, 587)
29	<	(61, 129)	64	_	(90, 730)	99	Г	(192, 719)	134	ж	(235, 19)
30	=	(61, 622)	65	`	(93, 267)	100	Д	(194, 205)	135	з	(235, 732)
31	>	(62, 372)	66	a	(93, 484)	101	Е	(194, 546)	136	н	(236, 39)
32	?	(62, 379)	67	b	(98, 338)	102	Ж	(197, 145)	137	й	(236, 712)
33	@	(66, 199)	68	c	(98, 413)	103	З	(197, 606)	138	к	(237, 297)
34	A	(66, 552)	69	d	(99, 295)	104	И	(198, 224)	139	л	(237, 454)

140	м	(238, 175)	145	с	(243, 664)	150	ц	(250, 14)	155	ы	(253, 540)
141	н	(238, 576)	146	т	(247, 266)	151	ч	(250, 737)	156	ь	(256, 121)
142	о	(240, 309)	147	у	(247, 485)	152	ш	(251, 245)	157	э	(256, 630)
143	п	(240, 442)	148	ф	(249, 183)	153	щ	(251, 506)	158	ю	(257, 293)
144	р	(243, 87)	149	х	(249, 568)	154	ъ	(253, 211)	159	я	(257, 458)

Задание 1. Зашифровать открытый текст на эллиптической кривой $E_{751}(1;1)$, где генерирующая точка $G = (0,1)$. Использовать алфавит, который приведен выше.

№ варианта	Открытый текст	Открытый ключ B	Значения случайных чисел k для букв открытого текста
1	передряга	(489, 468)	18, 15, 14, 18, 5, 10, 19, 14, 19
2	латышский	(179, 275)	15, 17, 12, 2, 2, 4, 8, 6, 17
3	регрессор	(425, 663)	6, 12, 16, 4, 9, 4, 19, 9, 18
4	симметрия	(179, 275)	11, 17, 18, 19, 16, 6, 12, 8, 2
5	уверовать	(425, 663)	6, 14, 5, 7, 12, 11, 4, 9, 19
6	терновник	(188, 93)	8, 14, 17, 17, 2, 10, 8, 2, 2
7	терпеливо	(725, 195)	17, 5, 4, 17, 13, 2, 17, 14, 19
8	ремонтный	(188, 93)	2, 2, 4, 18, 15, 19, 11, 2, 15
9	ренессанс	(725, 195)	2, 19, 4, 8, 2, 2, 16, 10, 2
10	репарация	(435, 663)	12, 11, 18, 7, 16, 18, 17, 2, 3
11	пролежень	(179, 275)	9, 5, 17, 2, 2, 2, 3, 17, 15
12	прокрутка	(618, 206)	10, 15, 16, 2, 3, 4, 2, 11, 16
13	прокопать	(489, 468)	3, 16, 17, 5, 16, 18, 3, 7, 15
14	отступить	(188, 93)	7, 9, 3, 8, 18, 18, 8, 11, 16
15	отставной	(286, 136)	5, 3, 3, 2, 4, 19, 2, 4, 10
16	отслужить	(16, 416)	2, 8, 4, 2, 6, 10, 3, 3, 18
17	отследить	(188, 93)	19, 2, 13, 5, 19, 5, 7, 8, 5
18	новенький	(425, 663)	19, 12, 13, 2, 12, 14, 19, 18, 12
19	нищенский	(489, 468)	2, 2, 7, 11, 19, 4, 2, 15, 6
20	никелевый	(568, 355)	9, 9, 2, 3, 8, 19, 6, 18, 9
21	низменный	(286, 136)	12, 5, 7, 17, 18, 2, 12, 10, 11
22	неэтичный	(489, 468)	14, 18, 11, 11, 6, 6, 17, 2, 5
23	мысленный	(346, 242)	6, 17, 18, 11, 18, 2, 4, 2, 12
24	муштровка	(618, 206)	5, 19, 8, 2, 5, 8, 15, 19, 6
25	латентный	(725, 195)	9, 10, 13, 2, 2, 12, 12, 5, 7
26	купальщик	(188, 93)	17, 17, 9, 12, 17, 7, 15, 7, 16
27	излечимый	(179, 275)	10, 14, 2, 2, 10, 10, 14, 3, 7
28	звездочка	(725, 195)	11, 17, 10, 10, 5, 2, 10, 19, 4
29	аберрация	(56, 419)	16, 2, 17, 19, 8, 4, 3, 2, 8
30	белиберда	(286, 136)	2, 9, 18, 2, 19, 4, 5, 11, 9

Задание 2. Дан шифртекст. Используя алфавит, приведенный выше, эллиптическую кривую $E_{751}(1; 1)$, где генерирующая точка $G = (0, 1)$ и секретный ключ b_n , найти открытый текст.

№ варианта	Секретный ключ n_b	Шифртекст
1	29	$\{(440, 539), (128, 672)\}; \{(489, 468), (282, 341)\};$ $\{(489, 468), (45, 720)\}; \{(72, 254), (227, 299)\};$ $\{(188, 93), (251, 506)\}; \{(72, 254), (319, 518)\};$ $\{(745, 210), (129, 659)\}; \{(286, 136), (515, 684)\};$ $\{(568, 355), (395, 414)\}$
2	25	$\{(72, 254), (397, 184)\}; \{(188, 93), (526, 412)\};$ $\{(188, 93), (328, 290)\}; \{(135, 82), (433, 47)\};$ $\{(179, 275), (711, 341)\}; \{(568, 355), (546, 670)\};$ $\{(16, 416), (734, 170)\}; \{(568, 355), (371, 14)\};$ $\{(596, 433), (604, 610)\}; \{(16, 416), (734, 170)\}$
3	40	$\{(188, 93), (573, 583)\}; \{(188, 93), (128, 79)\};$ $\{(425, 663), (703, 125)\}; \{(489, 468), (109, 200)\};$ $\{(568, 355), (348, 27)\}; \{(377, 456), (323, 657)\};$ $\{(72, 254), (399, 65)\}; \{(16, 416), (660, 275)\};$ $\{(179, 275), (267, 670)\}; \{(568, 355), (642, 53)\}$
4	34	$\{(618, 206), (426, 662)\}; \{(72, 254), (67, 667)\};$ $\{(286, 136), (739, 574)\}; \{(16, 416), (143, 602)\};$ $\{(618, 206), (313, 203)\}; \{(618, 206), (114, 607)\};$ $\{(618, 206), (438, 711)\}; \{(188, 93), (573, 168)\}$
5	41	$\{(283, 493), (314, 127)\}; \{(425, 663), (561, 140)\};$ $\{(568, 355), (75, 433)\}; \{(440, 539), (602, 627)\};$ $\{(188, 93), (395, 414)\}; \{(179, 275), (25, 604)\};$ $\{(72, 254), (47, 349)\}; \{(72, 254), (417, 137)\};$ $\{(188, 93), (298, 225)\}; \{(56, 419), (79, 111)\}$
6	44	$\{(377, 456), (367, 360)\}; \{(425, 663), (715, 398)\};$ $\{(188, 93), (279, 353)\}; \{(179, 275), (128, 79)\};$ $\{(568, 355), (515, 67)\}; \{(568, 355), (482, 230)\};$ $\{(377, 456), (206, 645)\}; \{(188, 93), (300, 455)\};$ $\{(489, 468), (362, 446)\}; \{(16, 416), (69, 510)\};$ $\{(425, 663), (218, 601)\}$
7	12	$\{(16, 416), (128, 672)\}; \{(56, 419), (59, 386)\};$ $\{(425, 663), (106, 24)\}; \{(568, 355), (145, 608)\};$ $\{(188, 93), (279, 398)\}; \{(425, 663), (99, 295)\};$ $\{(179, 275), (269, 187)\}; \{(188, 93), (395, 337)\};$ $\{(188, 93), (311, 68)\}; \{(135, 82), (556, 484)\};$ $\{(56, 419), (106, 727)\}; \{(16, 416), (307, 693)\}$
8	45	$\{(745, 210), (259, 401)\}; \{(568, 355), (606, 147)\};$ $\{(188, 93), (407, 82)\}; \{(56, 419), (739, 574)\};$ $\{(286, 136), (329, 447)\}; \{(425, 663), (520, 749)\};$ $\{(72, 254), (374, 315)\}; \{(188, 93), (149, 97)\};$ $\{(745, 210), (13, 134)\}; \{(440, 539), (235, 19)\};$ $\{(425, 663), (128, 79)\}$

9	32	{(188, 93), (623, 166)}; {(725, 195), (513, 414)}; {(346, 242), (461, 4)}; {(489, 468), (739, 574)}; {(725, 195), (663, 476)}; {(745, 210), (724, 522)}; {(725, 195), (663, 476)}; {(618, 206), (438, 40)}; {(286, 136), (546, 670)}; {(179, 275), (73, 72)}
10	18	{(179, 275), (269, 564)}; {(179, 275), (73, 72)}; {(440, 539), (189, 454)}; {(618, 206), (628, 458)}; {(568, 355), (660, 275)}; {(72, 254), (709, 595)}; {(745, 210), (12, 314)}; {(188, 93), (36, 664)}; {(618, 206), (530, 22)}; {(286, 136), (532, 50)}; {(425, 663), (660, 275)}; {(725, 195), (482, 230)}
11	27	{(745, 210), (185, 105)}; {(188, 93), (681, 385)}; {(377, 456), (576, 465)}; {(440, 539), (138, 298)}; {(745, 210), (520, 2)}; {(188, 93), (681, 385)}; {(286, 136), (282, 410)}; {(72, 254), (200, 721)}; {(72, 254), (643, 94)}; {(745, 210), (476, 315)}; {(440, 539), (724, 229)}
12	25	{(425, 663), (651, 191)}; {(188, 93), (177, 562)}; {(286, 136), (603, 562)}; {(440, 539), (588, 707)}; {(72, 254), (269, 187)}; {(56, 419), (49, 568)}; {(16, 416), (426, 662)}; {(425, 663), (557, 28)}; {(188, 93), (149, 97)}; {(179, 275), (711, 341)}
13	48	{(179, 275), (712, 186)}; {(725, 195), (395, 414)}; {(72, 254), (434, 136)}; {(425, 663), (251, 506)}; {(16, 416), (383, 340)}; {(745, 210), (102, 484)}; {(346, 242), (78, 271)}; {(179, 275), (712, 186)}; {(725, 195), (739, 574)}; {(346, 242), (78, 271)}
14	51	{(425, 663), (273, 481)}; {(188, 93), (85, 716)}; {(16, 416), (422, 162)}; {(283, 493), (36, 87)}; {(179, 275), (100, 364)}; {(188, 93), (298, 225)}; {(56, 419), (555, 303)}; {(745, 210), (100, 387)}; {(377, 456), (526, 412)}; {(286, 136), (316, 228)}; {(745, 210), (49, 183)}; {(179, 275), (428, 247)}
15	27	{(618, 206), (99, 456)}; {(425, 663), (31, 136)}; {(377, 456), (688, 741)}; {(425, 663), (636, 747)}; {(16, 416), (298, 526)}; {(188, 93), (356, 175)}; {(489, 468), (147, 390)}; {(346, 242), (546, 670)}; {(72, 254), (114, 144)}; {(377, 456), (25, 147)}
16	48	{(16, 416), (724, 522)}; {(489, 468), (719, 538)}; {(56, 419), (205, 372)}; {(72, 254), (628, 293)}; {(188, 93), (594, 337)}; {(440, 539), (588, 707)}; {(568, 355), (707, 556)}; {(489, 468), (719, 538)}; {(16, 416), (590, 376)}; {(56, 419), (612, 329)}; {(188, 93), (594, 337)}
17	51	{(56, 419), (739, 177)}; {(16, 416), (282, 410)}; {(425, 663), (221, 138)}; {(188, 93), (329, 447)}; {(286, 136), (235, 19)}; {(725, 195), (496, 31)}; {(56, 419), (236, 712)}; {(440, 539), (514, 662)}; {(377, 456), (323, 94)}; {(179, 275), (203, 324)}; {(568, 355), (197, 606)}

18	16	$\{(745, 210), (268, 597)\}; \{(725, 195), (310, 582)\};$ $\{(618, 206), (59, 365)\}; \{(440, 539), (371, 14)\};$ $\{(188, 93), (348, 27)\}; \{(72, 254), (434, 136)\};$ $\{(16, 416), (623, 166)\}; \{(188, 93), (235, 19)\};$ $\{(440, 539), (660, 275)\}; \{(188, 93), (434, 615)\};$ $\{(725, 195), (73, 679)\}; \{(188, 93), (642, 53)\}$
19	34	$\{(725, 195), (538, 325)\}; \{(725, 195), (176, 413)\};$ $\{(425, 663), (689, 670)\}; \{(346, 242), (652, 315)\};$ $\{(283, 493), (463, 736)\}; \{(16, 416), (744, 133)\};$ $\{(179, 275), (542, 351)\}; \{(56, 419), (298, 225)\};$ $\{(286, 136), (719, 538)\}; \{(568, 355), (319, 518)\};$ $\{(16, 416), (704, 46)\}$
20	25	$\{(725, 195), (329, 304)\}; \{(440, 539), (59, 386)\};$ $\{(618, 206), (543, 357)\}; \{(188, 93), (520, 749)\};$ $\{(489, 468), (585, 211)\}; \{(179, 275), (707, 556)\};$ $\{(596, 433), (419, 38)\}; \{(377, 456), (643, 94)\};$ $\{(188, 93), (385, 749)\}; \{(725, 195), (150, 355)\};$ $\{(725, 195), (197, 606)\}$
21	58	$\{(16, 416), (93, 484)\}; \{(489, 468), (531, 397)\};$ $\{(188, 93), (654, 102)\}; \{(489, 468), (218, 150)\};$ $\{(16, 416), (530, 729)\}; \{(425, 663), (295, 219)\};$ $\{(725, 195), (742, 299)\}; \{(188, 93), (367, 360)\};$ $\{(188, 93), (235, 732)\}; \{(618, 206), (251, 245)\};$ $\{(425, 663), (688, 10)\}$
22	50	$\{(179, 275), (326, 675)\}; \{(725, 195), (83, 378)\};$ $\{(440, 539), (340, 78)\}; \{(425, 663), (67, 84)\};$ $\{(425, 663), (620, 71)\}; \{(72, 254), (251, 245)\};$ $\{(568, 355), (75, 318)\}; \{(725, 195), (228, 271)\};$ $\{(188, 93), (734, 170)\}; \{(188, 93), (704, 705)\};$ $\{(286, 136), (235, 732)\}$
23	19	$\{(618, 206), (294, 595)\}; \{(188, 93), (13, 617)\};$ $\{(188, 93), (206, 106)\}; \{(188, 93), (67, 667)\};$ $\{(56, 419), (350, 184)\}; \{(440, 539), (275, 456)\};$ $\{(745, 210), (301, 17)\}; \{(346, 242), (588, 707)\};$ $\{(188, 93), (256, 121)\}; \{(425, 663), (209, 82)\};$ $\{(16, 416), (687, 660)\}$
24	54	$\{(188, 93), (295, 219)\}; \{(618, 206), (646, 706)\};$ $\{(440, 539), (573, 583)\}; \{(16, 416), (694, 581)\};$ $\{(179, 275), (585, 540)\}; \{(377, 456), (701, 570)\};$ $\{(618, 206), (67, 667)\}; \{(286, 136), (36, 664)\};$ $\{(72, 254), (727, 65)\}; \{(568, 355), (438, 40)\}$
25	55	$\{(725, 195), (9, 150)\}; \{(745, 210), (138, 453)\};$ $\{(56, 419), (36, 87)\}; \{(283, 493), (39, 580)\};$ $\{(377, 456), (515, 684)\}; \{(346, 242), (458, 261)\};$ $\{(283, 493), (105, 369)\}; \{(568, 355), (326, 675)\};$ $\{(425, 663), (529, 358)\}; \{(283, 493), (668, 409)\}$
26	24	$\{(16, 416), (150, 355)\}; \{(188, 93), (394, 20)\};$ $\{(725, 195), (13, 134)\}; \{(377, 456), (209, 669)\};$ $\{(56, 419), (514, 662)\}; \{(56, 419), (243, 87)\};$ $\{(618, 206), (719, 538)\}; \{(618, 206), (159, 13)\};$ $\{(618, 206), (326, 76)\}; \{(188, 93), (557, 28)\}$

27	43	$\{(440, 539), (279, 398)\}; \{(568, 355), (295, 219)\};$ $\{(16, 416), (724, 229)\}; \{(346, 242), (730, 240)\};$ $\{(72, 254), (334, 226)\}; \{(188, 93), (310, 169)\};$ $\{(72, 254), (36, 664)\}; \{(179, 275), (481, 369)\};$ $\{(188, 93), (236, 39)\}; \{(377, 456), (438, 711)\};$ $\{(377, 456), (307, 58)\}$
28	20	$\{(16, 416), (675, 505)\}; \{(72, 254), (611, 579)\};$ $\{(72, 254), (727, 686)\}; \{(489, 468), (39, 171)\};$ $\{(72, 254), (531, 354)\}; \{(568, 355), (36, 87)\};$ $\{(188, 93), (588, 44)\}; \{(618, 206), (70, 195)\};$ $\{(568, 355), (267, 81)\}; \{(56, 419), (525, 674)\}$
29	47	$\{(725, 195), (651, 560)\}; \{(425, 663), (147, 361)\};$ $\{(286, 136), (109, 551)\}; \{(440, 539), (90, 730)\};$ $\{(618, 206), (668, 342)\}; \{(745, 210), (109, 200)\};$ $\{(425, 663), (147, 361)\}; \{(72, 254), (228, 480)\};$ $\{(346, 242), (530, 22)\}$
30	50	$\{(16, 416), (726, 608)\}; \{(188, 93), (395, 337)\};$ $\{(440, 539), (163, 513)\}; \{(188, 93), (269, 187)\};$ $\{(725, 195), (177, 562)\}; \{(188, 93), (115, 509)\};$ $\{(188, 93), (734, 170)\}; \{(745, 210), (110, 622)\};$ $\{(179, 275), (576, 286)\}; \{(188, 93), (325, 297)\}$