

Bernd Köhler

Primzahlengenerator

Zweck Gesucht sind in aufsteigender Reihenfolge Primzahlen p mit $10 < p < 10^{10}$.

Theorie Folgender Satz ist die Grundlage des Verfahrens:

Satz: Es sei x eine natürliche Zahl und *nicht* Vielfaches einer Primzahl p (sie ist dann erst recht nicht Vielfaches einer anderen natürlichen Zahl und insbesondere keiner Primzahl) mit der Bedingung

$$p \leq \sqrt{x},$$

dann ist x ebenfalls eine Primzahl.

Die Zusatzbemerkung in der Klammer läßt sich wie folgt beweisen: Jede natürliche Zahl kann man als ein Produkt von Primzahlpotenzen darstellen (Fundamentalsatz der elementaren Zahlentheorie, hier ohne Beweis angeführt). Die „Primzahl“ p wäre also ein Vielfaches jener Primzahlen, also keine Primzahl!

Das Vielfache einer anderen Primzahl kann sie auch nicht sein: Es sei

$$x = np_1$$

$$x = mp_2 = (n+k)p_2; \quad n, k = 1, 2, 3, \dots$$

durch Division erhält man

$$1 = \frac{(n+k)p_2}{np_1}; \quad np_1 = np_2 + kp_2.$$

Es gibt nun zwei Fälle:

- a) $p_2 > p_1$: $n(p_1 - p_2) = kp_2$
Widerspruch!! Die linke Seite ist negativ, die rechte nicht!
- b) $p_2 < p_1$:
Widerspruch!! Die linke Seite ist immer gerade, die rechte nicht!

Beispiele: 37 ist Primzahl, denn sie ist nicht Vielfaches von 2, 3, 5. Für diese Primzahl gilt aber die Bedingung. Für 7 gilt sie nicht mehr.

49 ist keine Primzahl, obwohl die Bedingung erfüllt ist. Sie ist Vielfaches von 7. 243 ist auch keine Primzahl obwohl die Bedingung erfüllt ist, denn sie ist ebenfalls Vielfaches von 7. Vielfaches einer anderen (höheren) Primzahl kann sie laut Satz auch nicht sein. Durch Rechnung findet man: 243 ist nicht Vielfaches von 11, 13, 17. Für 17 ist bereits die Bedingung nicht mehr erfüllt.

Entwicklung eines Algorithmus

1. Ob x ein Vielfaches einer Primzahl p ist findet man durch Teilen mit geeigneten Zahlen heraus. Im Satz wird immer von

einer Primzahl p gesprochen. Diese ist aber nicht bekannt. Man wird also erst einmal x durch alle ungeraden Zahlen t teilen. Dann sind auch alle Primzahlen darunter.

2. Ist x ohne Rest teilbar, dann ist x bestimmt keine Primzahl und man erhöht sie um zwei (nächste auf x folgende ungerade Zahl) und fängt mit dem Teilen wieder von vorne an.

3. Es bleibt ein Rest R übrig. Es wird dann der Test $\sqrt{x} \geq t$ durchgeführt. Wird er mit nein beantwortet, ist x eine Primzahl. Andernfalls wird mit dem nächsten ungeraden Teiler fortgefahren.

4. Es gilt nun die Frage zu klären, ob man das „Erhöhen“ von x und t nicht durch ein schnelleres Verfahren ersetzen kann. Für x sollen deshalb als „Primzahlenanwärter“ nur solche Zahlen infrage kommen, die nicht gerade, nicht durch 3 teilbar (Quersumme) und nicht durch 5 teilbar sind (Endziffer 0 oder 5). Das sind jene Zahlen, die modulo $30 = 2 \cdot 3 \cdot 5$ die Reste $R = 1, 7, 11, 13, 17, 19, 23, 29, (31), (37), \dots$ haben. Die Differenzen d zwischen diesen Resten sind $6, 4, 2, 4, 2, 4, 6, 2, (6), \dots$

Die Zahl x muß also am Anfang auf ihren Rest R untersucht werden, damit die Erhöhungen mit der richtigen Zahl d beginnen.

Bei Rest R

R	1	7	11	13	17	19	23	29	(31)	(37)	(41)
wird erhöht um d	6	4	2	4	2	4	6	2	6	4	

5. Der erste Divisor ist 7, weil 2, 3, 5 nicht infrage kommen. Die erste zu untersuchende Zahl ist somit 11. Für die Erhöhung des Teilers t machen wir uns die Tatsache zunutze, daß jede Primzahl in der Form $6n \pm 1$ darstellbar ist, $n = 1, 2, 3, \dots$ Wir erhöhen also 7 abwechselnd um 4, 2, 4, 2, ... usw.

6. Der Test „Quersumme“ wird vom Programm vorgenommen. Ist die Zahl x durch 3 teilbar, wird sie vom Programm durch Abzählen von jeweils 2 entsprechend variiert werden. Andernfalls führt das Programm den Test „Rest“ aus und ordnet für die Erhöhung von x das richtige d zu.

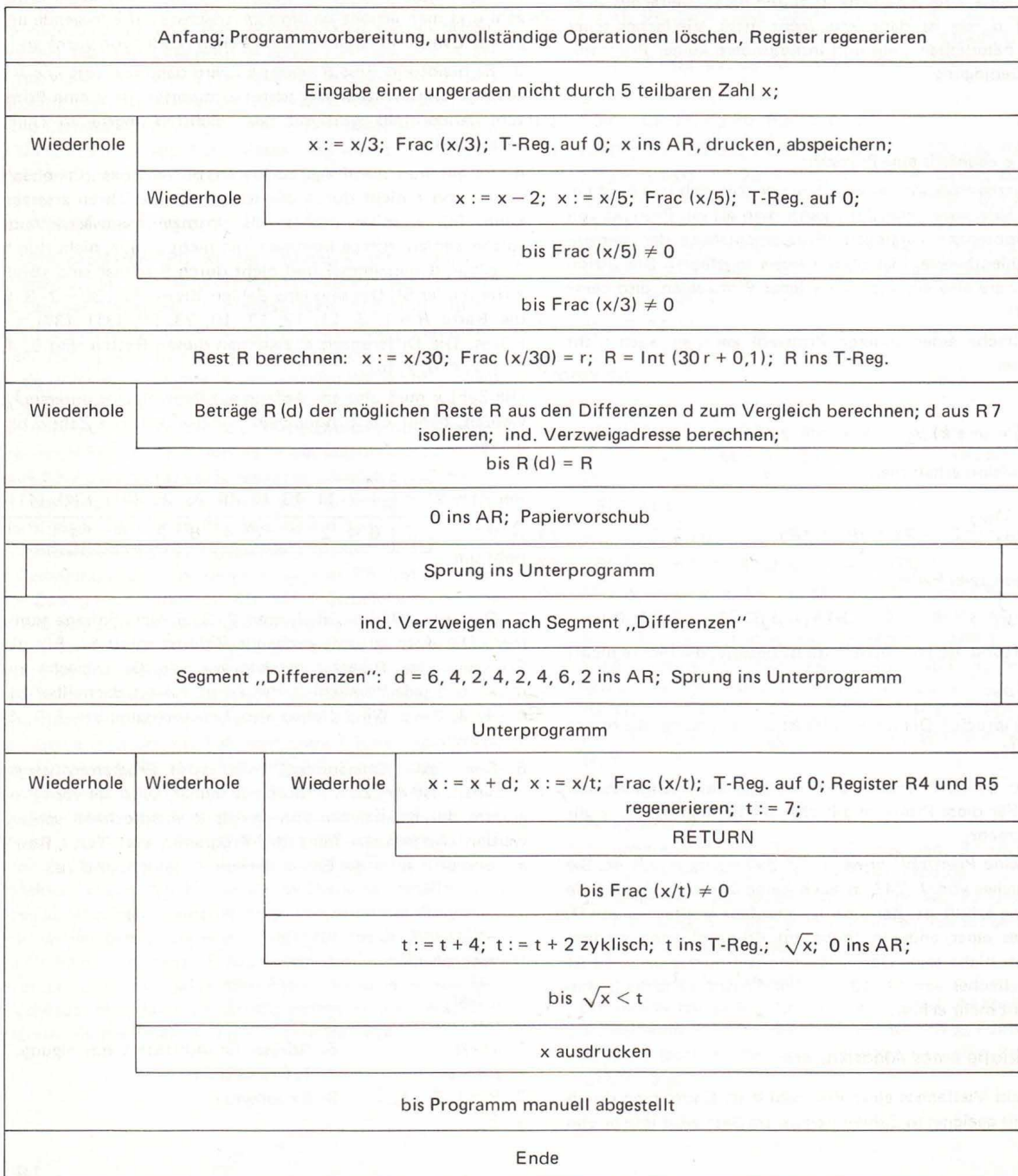
Speicherplan:

- T: belegt
- 0: frei
- 1: $x; x/t$
- 2: $t; t+d$
- 3: $R = 1, 7, 11, \dots$
- 4: 2
- 5: -2
- 6: Adresse für indirekte Verzweigung
- 7: 1, 642424621
- 8: Exponenten

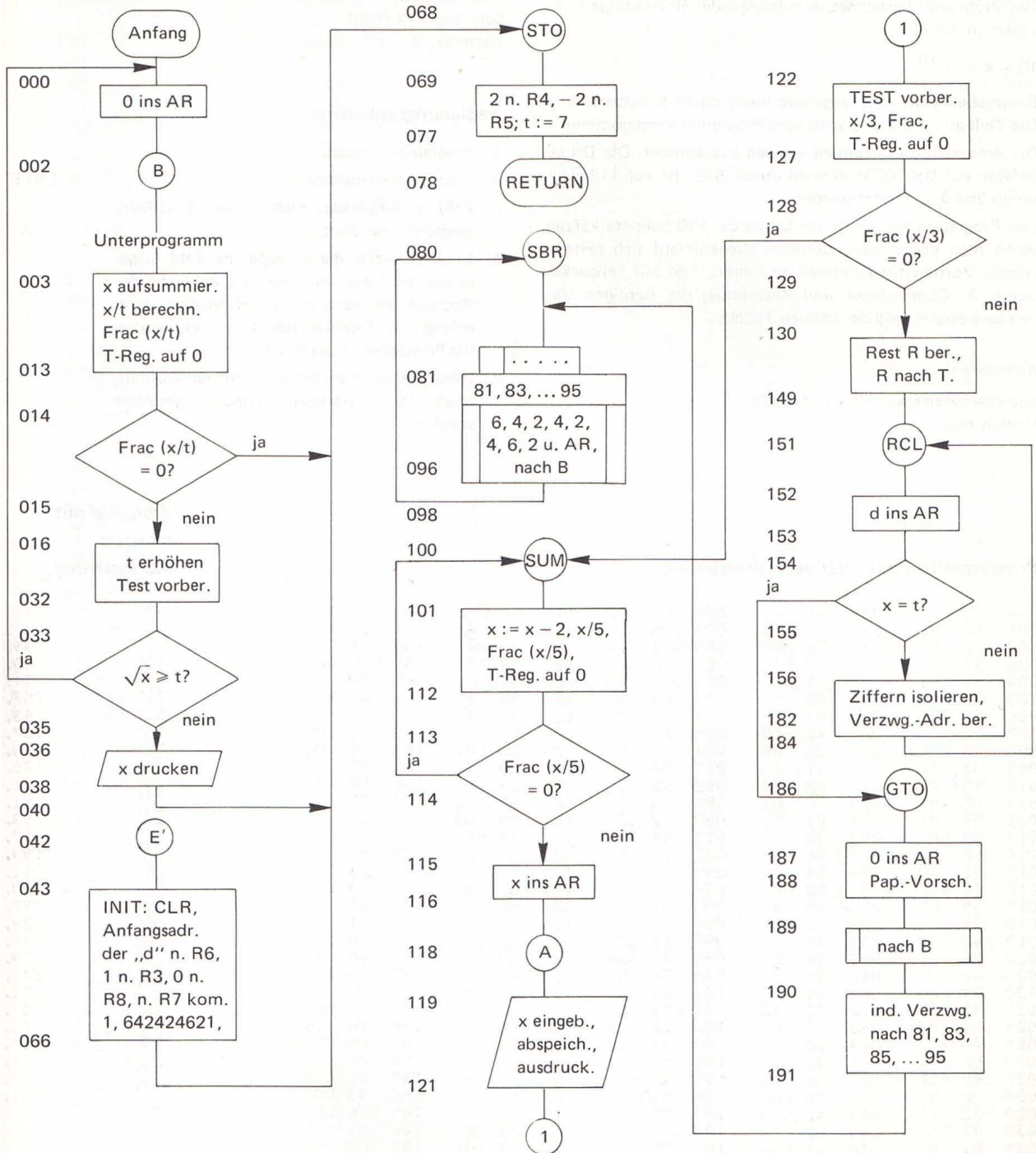
PSS	Label	Segment	abs. Adresse	080 SBR	Segment für die Differenzen d	079
				100 SUM	Variation von x	098
				118 A	Start	116
002	B	Unterprogramm	002	151 RCL	Ermittlung der indirekten Sprungadresse	149
042	E'	Initialisierung	044	186 GTO	Beginn der Rechnung	184
068	STO	$t = 7$ speichern	069			

Struktogramm

Hauptprogramm



Programmablaufplan



Programmbeschreibung

Das Programm berechnet in aufsteigender Reihenfolge Primzahlen im Bereich

$$10 < x < 10^{10}$$

Eingegeben wird eine ungerade nicht durch 5 teilbare Zahl. Die Teilbarkeit durch 3 wird vom Programm vorgenommen.

Die ermittelten Primzahlen werden ausgedruckt. Die Druckbefehle auf 038 (039) können durch R/S, die auf 119 (117) durch 2nd Nop ersetzt werden.

Das Programm ließe sich um bis zu ca. 120 Schritte kürzen, wenn man etwas mehr Unbequemlichkeit auf sich nehmen würde: Vorbereitung manuell ausführen, Test auf Teilbarkeit durch 3 (Quersumme) und Zuordnung der richtigen Verzweigungsadresse mittels der kleinen Tabelle.

Kenndaten:

Speicherbereichsverteilung: 479/59
Modul: nein

Drucker: ja
Magnetkarten: 1
Schritte: 192 (189)
Speicher: 8

Bedienungsanleitung

- 1 Programm einlesen
- 2 Programm vorbereiten 2nd E'
- 3 Zahl x (ungerade, nicht durch 5 teilbar) eingeben und Start A
- 4 Es wird zuerst die eingegebene Zahl ausgedruckt und evtl. eine weitere Zahl, die der Rechner bei seinem Test ermittelte, dann erfolgt der Papiervorschub und es werden die Primzahlen ausgedruckt
- 5 Wenn genug Primzahlen ermittelt wurden, muß das Programm manuell gestoppt werden.

Beispiele mit relativer Adressierung

Programmliste mit relativer Adressierung

000	00	0	039	61	GTO	078	92	RTH	117	76	LBL	156	43	RCL	7.	131.
001	76	LBL	040	42	STD	079	76	LBL	118	11	A	157	07	07	13.	137.
002	12	B	041	76	LBL	080	71	SBR	119	99	PRT	158	65	x	11.	139.
003	44	SUM	042	10	E'	081	06	6	120	42	STD	159	69	DP	13.	149.
004	01	01	043	25	CLR	082	12	B	121	01	01	160	28	28	17.	151.
005	43	RCL	044	08	8	083	04	4	122	55	+	161	43	RCL	19.	157.
006	01	01	045	01	1	084	12	B	123	03	3	162	08	08	23.	163.
007	55	+	046	42	STD	085	02	2	124	95	=	163	22	INV	29.	167.
008	43	RCL	047	06	06	086	12	B	125	22	INV	164	28	LDG	31.	173.
009	92	02	048	01	1	087	04	4	126	59	INT	165	95	=	37.	179.
010	95	=	049	42	STD	088	12	B	127	29	CP	166	59	INT	41.	181.
011	22	INV	050	03	03	089	02	2	128	67	EQ	167	55	+	43.	191.
012	59	INT	051	01	1	090	12	B	129	44	SUM	168	01	1	47.	193.
013	29	CP	052	93	.	091	04	4	130	43	RCL	169	00	0	53.	197.
014	67	EQ	053	06	6	092	12	B	131	01	01	170	95	=	59.	199.
015	42	STD	054	04	4	093	06	6	132	55	+	171	22	INV	61.	211.
016	43	RCL	055	02	2	094	12	B	133	03	3	172	59	INT	67.	223.
017	05	05	056	04	4	095	02	2	134	00	0	173	65	x	71.	227.
018	94	+/-	057	02	2	096	12	B	135	95	=	174	01	1	73.	229.
019	42	STD	058	04	4	097	61	GTO	136	22	INV	175	00	0	79.	233.
020	05	05	059	06	6	098	71	SBR	137	59	INT	176	95	=	83.	239.
021	44	SUM	060	02	2	099	76	LBL	138	65	x	177	44	SUM	89.	241.
022	04	04	061	01	1	100	44	SUM	139	03	3	178	03	03	97.	251.
023	43	RCL	062	42	STD	101	02	2	140	00	0	179	69	DP	101.	257.
024	04	04	063	07	07	102	22	INV	141	85	+	180	26	26	103.	263.
025	44	SUM	064	00	0	103	44	SUM	142	93	.	181	69	DP	107.	269.
026	02	02	065	42	STD	104	01	01	143	01	1	182	26	26	109.	271.
027	43	RCL	066	08	08	105	43	RCL	144	95	=	183	61	GTO	113.	277.
028	02	02	067	76	LBL	106	01	01	145	52	EE	184	43	RCL	127.	281.
029	32	XIT	068	42	STD	107	55	+	146	22	INV	185	76	LBL		
030	43	RCL	069	02	2	108	05	5	147	52	EE	186	61	GTO		
031	01	01	070	42	STD	109	95	=	148	59	INT	187	00	0		
032	34	FX	071	04	04	110	22	INV	149	32	XIT	188	98	ADV		
033	77	GE	072	94	+/-	111	59	INT	150	76	LBL	189	12	B		
034	00	00	073	42	STD	112	29	CP	151	43	RCL	190	83	GD*		
035	00	00	074	05	05	113	67	EQ	152	43	RCL	191	06	06		
036	43	RCL	075	07	7	114	44	SUM	153	03	03	192	00	0		
037	01	01	076	42	STD	115	43	RCL	154	67	EQ	193	00	0		
038	99	PRT	077	02	02	116	01	01	155	61	GTO					

Beispiele mit
absoluter Adressierung

Programmliste mit absoluter Adressierung

000	00	0	040	61	GTD	080	12	B	120	55	+	160	08	08	7.
001	76	LBL	041	00	00	081	04	4	121	03	3	161	22	INV	
002	12	B	042	69	69	082	12	B	122	95	=	162	28	LDG	11.
003	44	SUM	043	76	LBL	083	02	2	123	22	INV	163	95	=	13.
004	01	01	044	10	E*	084	12	B	124	59	INT	164	59	INT	17.
005	43	RCL	045	25	CLK	085	04	4	125	29	CP	165	55	+	19.
006	01	01	046	07	7	086	12	B	126	67	EQ	166	01	1	23.
007	55	+	047	09	9	087	02	2	127	00	00	167	00	0	29.
008	43	RCL	048	42	STD	088	12	B	128	98	98	168	95	=	31.
009	02	02	049	06	06	089	04	4	129	43	RCL	169	22	INV	37.
010	95	=	050	01	1	090	12	B	130	01	01	170	59	INT	41.
011	22	INV	051	42	STD	091	06	6	131	55	+	171	65	x	43.
012	59	INT	052	03	03	092	12	B	132	03	3	172	01	1	47.
013	39	CP	053	01	1	093	02	2	133	00	0	173	00	0	53.
014	67	EQ	054	93	.	094	12	B	134	95	=	174	95	=	59.
015	00	00	055	06	6	095	61	GTD	135	22	INV	175	44	SUM	61.
016	69	69	056	04	4	096	00	00	136	59	INT	176	03	03	67.
017	43	RCL	057	02	2	097	79	79	137	65	x	177	69	DP	71.
018	05	05	058	04	4	098	02	2	138	03	3	178	26	26	73.
019	94	+/-	059	02	2	099	22	INV	139	00	0	179	69	DP	79.
020	42	STD	060	04	4	100	44	SUM	140	85	+	180	26	26	83.
021	05	05	061	06	6	101	01	01	141	93	.	181	61	GTD	89.
022	44	SUM	062	02	2	102	43	RCL	142	01	1	182	01	01	97.
023	04	04	063	01	1	103	01	01	143	95	=	183	49	49	101.
024	43	RCL	064	42	STD	104	55	-	144	52	EE	184	00	0	103.
025	04	04	065	07	07	105	05	5	145	22	INV	185	98	HDV	107.
026	44	SUM	066	00	0	106	95	=	146	52	EE	186	12	B	109.
027	02	02	067	42	STD	107	22	INV	147	59	INT	187	83	DD+	113.
028	43	RCL	068	08	08	108	59	INT	148	32	XIT	188	06	06	127.
029	02	02	069	02	2	109	29	CP	149	43	RCL	189	00	0	131.
030	32	XIT	070	42	STD	110	67	EQ	150	03	03	190	00	0	137.
031	43	RCL	071	04	04	111	00	00	151	67	EQ	191	00	0	139.
032	01	01	072	94	+/-	112	98	98	152	01	01	192	00	0	149.
033	34	FX	073	42	STD	113	43	RCL	153	84	84	193	00	0	151.
034	77	GE	074	05	05	114	01	01	154	43	RCL	194	00	0	157.
035	00	00	075	07	7	115	76	LBL	155	07	07	195	00	0	163.
036	00	00	076	42	STD	116	11	R	156	65	x	196	00	0	167.
037	43	RCL	077	02	02	117	99	PRT	157	69	DP	197	00	0	173.
038	01	01	078	92	RTN	118	42	STD	158	26	28	198	00	0	179.
039	99	PRT	079	06	6	119	01	01	159	43	RCL				181.

258967.

258967.

258971.

258977.