College Cryptografie

Cursusjaar 2003

Analyse van Codes

31 januari 2003

Known plaintext

Luiheid

Isolog

Monoalfabetisch karakter

Vercijferde code

Periodiek additief

Latente herhalingen

Long subtractors

ONDERWERPEN

Combineer herhalingen in klaartekst met herhalingen in code

1.	contraires à la presente forme de gouvernement que	3317 648 6 96 510 2146 2591 1814 1108 1428 1608 1476 1094
2.	sans aucune forme de proces	2769 326 952 110 1814 1108 2348
3.	que cette forme de gouvernement renfermoit	3000 941 1814 101 1428 1608 1276 2160
4.	donnee elle même la presente forme de gouvernement elle sauroit aussi le mieux	568 796 975 893 1075 1792 2146 2591 1814 1696 1428 1502 1476 975 604 2170 2021 428 604 1179

presente = 2146 2591 forme = 1814 el = 975 le = 893, 604

Known plaintext

- 15 juni 1918 aan het Oostenrijks-Italiaans front
  nieuwe code met 1000 groepen van 3 letters duikt op
- Cryptoanalist (later generaal) Luigi Sacco merkt op:
  berichten van radiostation op de Col della Guardia Conegliano
  bevatten klein aantal codegroepen met hoge frequentie
- 20 juni zelfs twee telegrammen met identiek slot
  492 073 065 834 729 589 255 073 255 834 729 264

- 20 juni twee telegrammen met identiek slot

492	073	065	834	729	589	255	073	255	834	729	264
R	A	D	I	O	S	T	A	T	I	O	N

- de fout: reductie van de code tot monoalfabetische substitutie door alleen de codegroepen voor de letters te benutten
- gevolgen:
  - delen van berichten ontcijferbaar
  - betekenis tussenliggende groepen te raden
  - binnen 6 dagen is de code grotendeels gebroken

Een *isolog* is een parallelle vercijfering

- 11 maart 1918 – 00:00 uur
  Duitsers vervangen de KRU-code door de Schlüßelheft

- Op dezelfde dag onderschept door afluisterpost Souilly:

  1. 00:40 X2 an ÄN: 00:25 CHI-13 845 422 373 792 240
     245 068 652 781 245 659 659 504

  2. 12:52 ÄN an X2: CHI-13 OS RGV KZD

  3. 12:57 X2 an ÄN: 00:25 CHI-14 UYC REM KUL RHI KWZ
     RLF RNQ KRD RVJ UOB KUU UQX UFQ RQK

Tweede bericht luidt

```
12:52 ÄN an X2: CHI-13 OS RGV KZD
```

Bekend van de KRU-code is

OS	=	Ohne Sinn
RGV	=	alte
KZD	=	Kode(?)

Leg (slot) eerste en derde bericht naast elkaar

RLF	RNQ	KRD	RVJ	UOB	KUU	UQX	UFQ		RQK
h	i	r	sch		w	i	tt		e
240	245	068	652		781	245	659	659	504

Fout: parallelle vercijfering geeft entree in nieuwe code

CYTVW UEYNY IUWUE YBETY MUIUF OWCWI CYTEW RXAVU LUYIX
ULFMU IUZEN MJYYF DURVZ ENMWO GBWOI DBEBG HIRAD IFMRE
ATJYY FDURV ZENMW OGBXI IFDIF MJYYF DURVZ ENMWO GBFYY
CXIIF DIFMB ETYKO MWJYY FDURV ZENMW OGBMI VIDIF MKOZK
JYYFD URVNO GWWOG BXITQ DIFMF AFPJY YFDUR VNOGU WOGBK
EER

Bericht – 1

CYTVW UEYNY IUWUE YCYTV MUIUX EUSKU WFWUE YMUIU PEBSQ
OTITU XPXAV UWIGC CAZGQ IQGRO WNCYT VHAWH MYYIK OZKKI
QBLAW LKUWF BETYT OGZMU IUCAR YTOQI XYTND IDKBI EICYT
VCAZG QIQGR OWNTO QIQEU MXYMF NYCOM EBQLU RBZEA ZDUQU
RUWMX ULF

Bericht – 2

Monoalfabetisch karakter

CYTVW UEYNY IUWUE YBETY MUIUF OWCWI CYTEW RXAVU LUYIX
ULFMU IUZEN MJYYF DURVZ ENMWO GBWOI DBEBG HIRAD IFMRE
ATJYY FDURV ZENMW OGBXI IFDIF MJYYF DURVZ ENMWO GBFYY
CXIIF DIFMB ETYKO MWJYY FDURV ZENMW OGBMI VIDIF MKOZK
JYYFD URVNO GWWOG BXITQ DIFMF AFPJY YFDUR VNOGU WOGBK
EER

Bericht – 1

CYTVW UEYNY IUWUE YCYTV MUIUX EUSKU WFWUE YMUIU PEBSQ
OTITU XPXAV UWIGC CAZGQ IQGRO WNCYT VHAWH MYYIK OZKKI
QBLAW LKUWF BETYT OGZMU IUCAR YTOQI XYTND IDKBI EICYT
VCAZG QIQGR OWNTO QIQEU MXYMF NYCOM EBQLU RBZEA ZDUQU
RUWMX ULF

Bericht – 2

Monoalfabetisch karakter

CYTV WUEY NYIU WUEY BETY MUIU FOWC WICY TEWR XAVU LUYI
XULF MUIU ZENM JYYF DURV ZENM WOGB WOID BEBG HIRA DIFM
REAT JYYF DURV ZENM WOGB XIIF DIFM JYYF DURV ZENM WOGB
FYYC XIIF DIFM BETY KOMW JYYF DURV ZENM WOGB MIVI DIFM
KOZK JYYF DURV NOGW WOGB XITQ DIFM FAFP JYYF DURV NOGU
WOGB KEER

Bericht - 1

CYTV WUEY NYIU WUEY CYTV MUIU XEUS KUWF WUEY MUIU PEBS
QOTI TUXP XAVU WIGC CAZG QIQG ROWN CYTV HAWH MYYI KOZK
KIQB LAWL KUWF BETY TOGZ MUIU CARY TOQI XYTN DIDK BIEI
CYTV CAZG QIQG ROWN TOQI QEUM XYMF NYCO MEBQ LURB ZEAZ
DUQU RUWM XULF

Bericht - 2

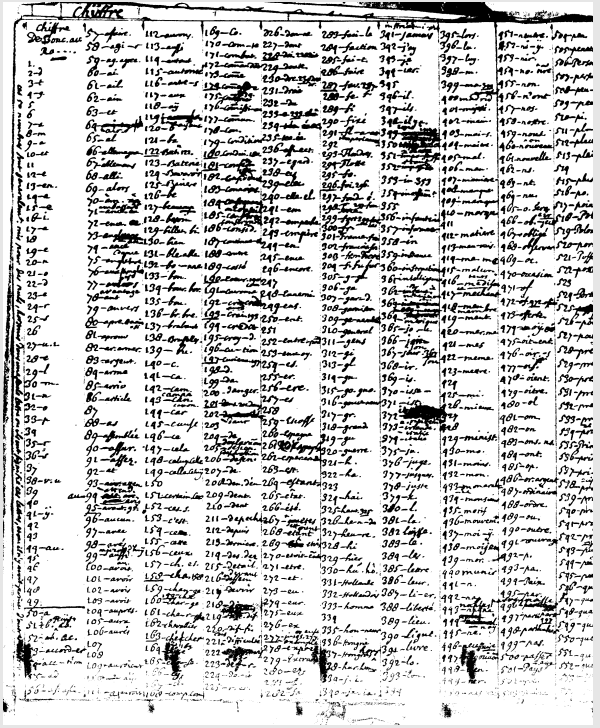
Monoalfabetisch karakter

CYTV WUEY NYIU WUEY BETY MUIU FOWC WICY TEWR XAVU LUYI
XULF MUIU ZENM JYYF DURV ZENM WOGB WOID BEBG HIRA DIFM
REAT JYYF DURV ZENM WOGB XIIF DIFM JYYF DURV ZENM WOGB
FYYC XIIF DIFM BETY KOMW JYYF DURV ZENM WOGB MIVI DIFM
KOZK JYYF DURV NOGW WOGB XITQ DIFM FAFP JYYF DURV NOGU
WOGB KEER

Bericht - 1

CYTV WUEY NYIU WUEY CYTV MUIU XEUS KUWF WUEY MUIU PEBS
QOTI TUXP XAVU WIGC CAZG QIQG ROWN CYTV HAWH MYYI KOZK
KIQB LAWL KUWF BETY TOGZ MUIU CARY TOQI XYTN DIDK BIEI
CYTV CAZG QIQG ROWN TOQI QEUM XYMF NYCO MEBQ LURB ZEAZ
DUQU RUWM XULF

Bericht - 2



Abel Tasien d'Alonne

William Blencowe

Twee codebrekers

additief/subtractor beschermt tegen ‘monoalfabetische’ aanval

codegroepen	12345	62019	83315	...
additief	36280	14600	03028	...
encicode	48525	76619	86333	...

of

codegroepen	12345	62019	83315	...
subtractor	36280	14600	03028	...
encicode	86165	58419	80397	...

additief/subtractor onbelangrijk voor oplossen

code	12345			code	12345
additief	36280	← complement →		subtractor	74820
encicode	48525			encicode	48525

volgorde operanden onbelangrijk voor oplossen

encicode	48525			additief	36280
additief	36280			encicode	48525
code	12345	← complement →		code	98765

Typen additief/subtractor

- lang (Duits: Zahlenwurm, limiet = one time pad)
- periodiek
- stuksgewijs (gestuurd door indicatorgroepen)

Behandeld wordt het breken van

- periodiek additief/subtractor Midway-oefening
- lang additief/subtractor

Technieken voor breken vercijferde code

- plaats materiaal in *diepte*
  uitlijnen van cryptogrammen zodanig dat groepen vercijferd met hetzelfde additief/subtractor onder elkaar staan

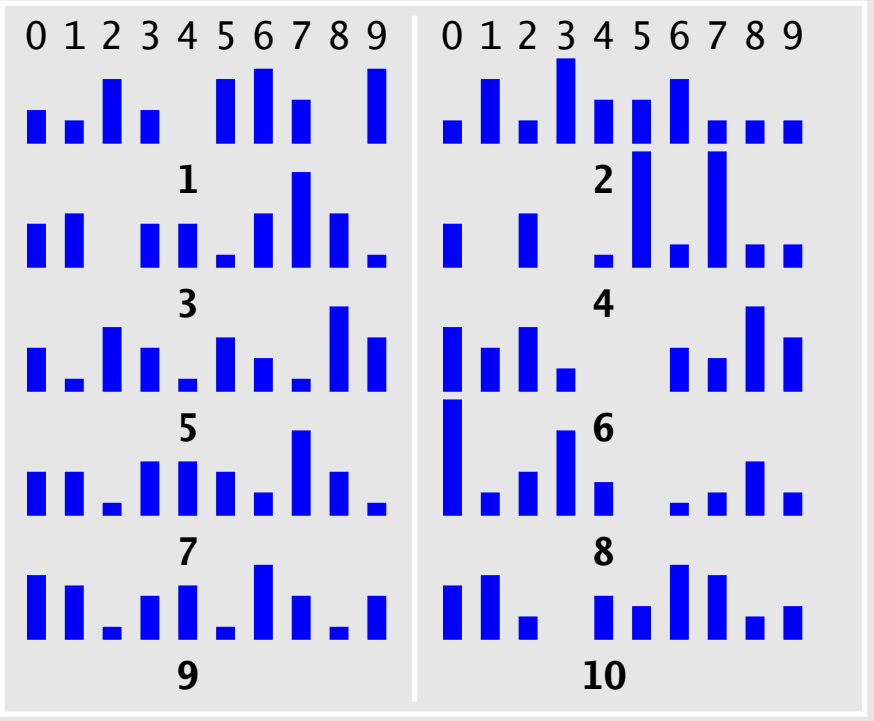
- beperkingen in constructie code benutten

  - alle codegroepen 00000–24999
    gevolg: beperking op eerste twee cijfers
  - geen 0 in subtractor
    gevolg: altijd encicode-cijfer ≠ code-cijfer

- vercijfering:
  letters → dinomes
  (b.v. A = 23, etc.)

- additief:
  10-cijferige reeks
  57 61 82 34 90

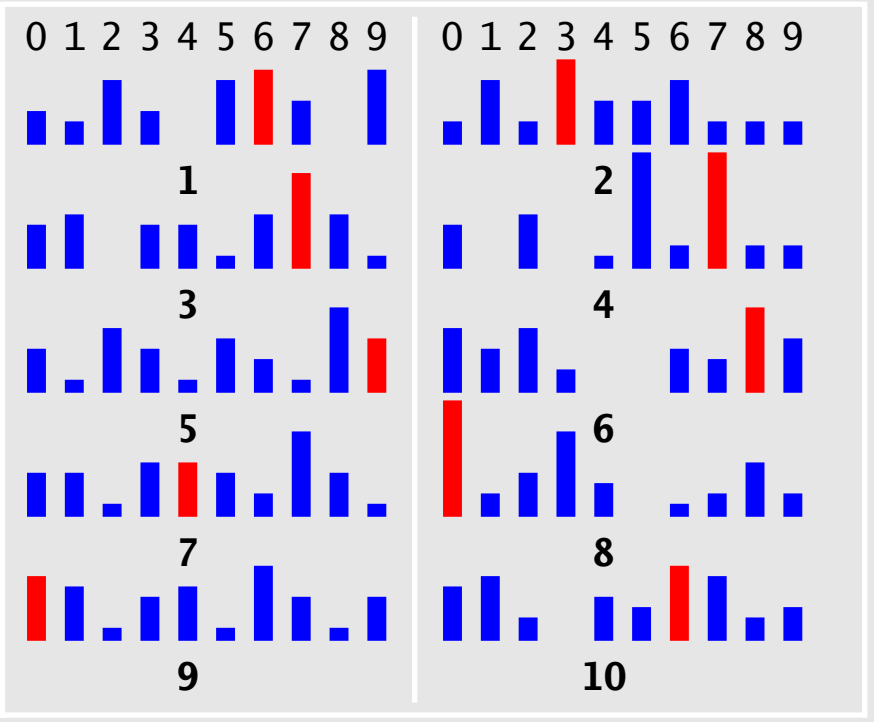
tellingen voor periode 10



Periodiek additief

- gevonden additief:
  63 77 98 40 06
- werkelijk additief:
  57 61 82 34 90
- verschil
  16 16 16 16 16

tellingen voor periode 10



Periodiek additief

Herhaling uit fase met additief

74	31	89	60	25	12	74	31	89	60	25	12	74	31	89	60	(a) additief
D	I	V	IS	ION	HE	A	D	Q	U	AR	TER	S	COM	M	..	(p) klaar
31	54	04	59	58	53	11	31	70	03	16	96	88	20	68	..	(c) cijfer
05	85	83	19	73	65	85	62	59	63	31	08	52	51	47	..	(e) encicode
ENT	TO	D	I	V	IS	ION	HE	A	D	Q	U	AR	TER	S	F	(p) klaar
30	02	31	54	04	59	58	53	11	31	70	03	16	96	88	46	(c) cijfer
04	33	10	14	29	61	22	84	90	91	95	15	80	27	67	06	(e) encicode

Herhaling uit fase met additief

74	31	89	60	25	12	74	31	89	60	25	12	74	31	89	60	(a) additief
D	I	V	IS	ION	HE	A	D	Q	U	AR	TER	S	COM	M	..	(p) klaar
31	54	04	59	58	53	11	31	70	03	16	96	88	20	68	..	(c) cijfer
05	85	83	19	73	65	85	62	59	63	31	08	52	51	47	..	(e) encicode
ENT	TO	D	I	V	IS	ION	HE	A	D	Q	U	AR	TER	S	F	(p) klaar
30	02	31	54	04	59	58	53	11	31	70	03	16	96	88	46	(c) cijfer
04	33	10	14	29	61	22	84	90	91	95	15	80	27	67	06	(e) encicode

bereken verschillen $\delta_i = e_{i+12} - e_i$

$$\delta_i = (c_{i+12} + a_{i+12}) - (c_i + a_i) = c_{i+12} - c_i$$

Verschillen δ_i

74	31	89	60	25	12	74	31	89	60	25	12	74	31	89	60	(a) additief
D	I	V	IS	ION	HE	A	D	Q	U	AR	TER	S	COM	M	..	(p) klaar
31	54	04	59	58	53	11	31	70	03	16	96	88	20	68	..	(c) cijfer
05	85	83	19	73	65	85	62	59	63	31	08	52	51	47	..	(e) encicode
						80	87	76	54	68	43	77	99	98	..	(d) verschil
ENT	TO	D	I	V	IS	ION	HE	A	D	Q	U	AR	TER	S	F	(p) klaar
30	02	31	54	04	59	58	53	11	31	70	03	16	96	88	46	(c) cijfer
04	33	10	14	29	61	22	84	90	91	95	15	80	27	67	06	(e) encicode
..	..	..	..	..	..	28	51	80	87	76	54	68	43	77	15	(d) verschil

Additief berekenen

ab	cd	ef	gh	ij	kl	ab	cd	ef	gh	ij	kl	ab	cd	ef
D	I	V	IS	ION	HE	A	D	Q	U	AR	TER	S		
05	85	83	19	73	65	85	62	59	63	31	08	52		
		D	I	V	IS	ION	HE	A	D	Q	U	AR	TER	S
		10	14	29	61	22	84	90	91	95	15	80	27	67

- D + ab = 05 en D + ef = 10 → ef = ab + 15
- kies aftelpunt ab = 00 dan ef = 15
- Q + ef = 59 en Q + ij = 95 → ij = ef + 46 = 51, enz.
- oplossing 00 67 15 96 51 48 equivalent 74 31 89 60 25 12

Oplosmethode

- arrangeer het materiaal *in diepte*
- herhalingen binnen kolom goede kandidaten volgende stap
- kies een groep als kolomadditief en *reduceer* kolom ermee
- herhaal voor alle kolommen
- stel eenzelfde gereduceerde groep staat in twee kolommen
- *hoop* dat het om dezelfde codegroep gaat
  en breng de twee kolommen hiermee op een noemer

	A	B	C	D	E	F	G	..
1	31892	64437	12991	82384	45306	87882	91445	..
2		54906	22775	85570	16687	87419	08502	..
3			12244	95354	19873	58790	06328	..
4	67072	80559	33541	73774	31360	46739	78358	..
5	45492	57229	26844	85622	53700	89693	06791	..
6	34810	80186	40608	87917	12449	72536	14722	..
7	69256	54358	34948	13287	32231	89664	01580	..
8	23791	41612	49942	07239	37344	87419	04858	..
9	47200	46805	11247	07527	24255	41314	91445	..
10	46921	44081	33541	11003	47580	87882	91445	..
11	24367	76140	02646	14862	02331	41314	91445	..
12	53665	80186	42669	11003	47700	87419	70333	..
13	44882	60353	21048	70323	12780	54257	64484	..
14	75050	98409	07744	20002	18551	45738	06328	..
15	65502	58906	33541	07682	47551	43823	92842	..

Long subtractors

	A	B	C	D	E	F	G	..
1	31892	64437	12991	82384	45306	87882	91445	..
2		54906	22775	85570	16687	87419	08502	..
3			12244	95354	19873	58790	06328	..
4	67072	80559	33541	73774	31360	46739	78358	..
5	45492	57229	26844	85622	53700	89693	06791	..
6	34810	80186	40608	87917	12449	72536	14722	..
7	69256	54358	34948	13287	32231	89664	01580	..
8	23791	41612	49942	07239	37344	87419	04858	..
9	47200	46805	11247	07527	24255	41314	91445	..
10	46921	44081	33541	11003	47580	87882	91445	..
11	24367	76140	02646	14862	02331	41314	91445	..
12	53665	80186	42669	11003	47700	87419	70333	..
13	44882	60353	21048	70323	12780	54257	64484	..
14	75050	98409	07744	20002	18551	45738	06328	..
15	65502	58906	33541	07682	47551	43823	92842	..

Long subtractors

	B	C	D	F			G	
1	80186	33541	11003	87882	87419	41314	91445	06328
1	64437	12991	82384	87882	87882	87882	91445	91445
2	54906	22775	85570	87419	87419	87419	08502	08502
3		12244	95354	58790	58790	58790	06328	06328
4	80559	33541	73774	46739	46739	46739	78358	78358
5	57229	26844	85622	89693	89693	89693	06791	06791
6	80186	40608	87917	72536	72536	72536	14722	14722
7	54358	34948	13287	89664	89664	89664	01580	01580
8	41612	49942	07239	87419	87419	87419	04858	04858
9	46805	11247	07527	41314	41314	41314	91445	91445
10	44081	33541	11003	87882	87882	87882	91445	91445
11	76140	02646	14862	41314	41314	41314	91445	91445
12	80186	42669	11003	87419	87419	87419	70333	70333
13	60353	21048	70323	54257	54257	54257	64484	64484
14	98409	07744	20002	45738	45738	45738	06328	06328
15	58906	33541	07682	43823	43823	43823	92842	92842

Long subtractors

	B	C	D	F			G	
1	80186	33541	11003	87882	87419	41314	91445	06328
1	84351	89450	71381	00000	00473	46578	00000	95127
2	74820	99234	74577	00637	00000	46105	17167	02284
3		89703	84351	71918	71381	17486	15983	00000
4	00473	00000	62771	69957	69320	05425	87913	72030
5	77143	93303	74629	02811	02284	48389	15356	00473
6	00000	17167	76914	95754	95127	31222	23387	18404
7	74272	01407	02284	02882	02255	48350	10145	05262
8	61536	16401	96236	00637	00000	46105	13413	08530
9	66729	88706	96524	64532	64905	00000	00000	95127
10	64905	00000	00000	00000	00473	46578	00000	95127
11	96064	79105	03869	64532	64905	00000	00000	95127
12	00000	19128	00000	00637	00000	46105	89998	74015
13	80277	98507	69320	77475	77848	13943	73049	68166
14	18323	74203	19009	68956	68329	04424	15983	00000
15	78820	00000	96689	66041	66414	02519	01407	96524

Long subtractors

	B	C	D	F			G	
1	80186	33541	11003	87882	87419	41314	91445	06328
1	84351	89450	71381	00000	00473	46578	00000	95127
2	74820	99234	74577	00637	00000	46105	17167	02284
3		89703	84351	71918	71381	17486	15983	00000
4	00473	00000	62771	69957	69320	05425	87913	72030
5	77143	93303	74629	02811	02284	48389	15356	00473
6	00000	17167	76914	95754	95127	31222	23387	18404
7	74272	01407	02284	02882	02255	48350	10145	05262
8	61536	16401	96236	00637	00000	46105	13413	08530
9	66729	88706	96524	64532	64905	00000	00000	95127
10	64905	00000	00000	00000	00473	46578	00000	95127
11	96064	79105	03869	64532	64905	00000	00000	95127
12	00000	19128	00000	00637	00000	46105	89998	74015
13	80277	98507	69320	77475	77848	13943	73049	68166
14	18323	74203	19009	68956	68329	04424	15983	00000
15	78820	00000	96689	66041	66414	02519	01407	96524

Long subtractors

	B	C	D	F			G	
1	80186	33541	11003	87882	87419	41314	91445	06328
1	84351	89450	71381	00000	00473	46578	00000	95127
2	74820	99234	74577	00637	00000	46105	17167	02284
3		89703	84351	71918	71381	17486	15983	00000
4	00473	00000	62771	69957	69320	05425	87913	72030
5	77143	93303	74629	02811	02284	48389	15356	00473
6	00000	17167	76914	95754	95127	31222	23387	18404
7	74272	01407	02284	02882	02255	48350	10145	05262
8	61536	16401	96236	00637	00000	46105	13413	08530
9	66729	88706	96524	64532	64905	00000	00000	95127
10	64905	00000	00000	00000	00473	46578	00000	95127
11	96064	79105	03869	64532	64905	00000	00000	95127
12	00000	19128	00000	00637	00000	46105	89998	74015
13	80277	98507	69320	77475	77848	13943	73049	68166
14	18323	74203	19009	68956	68329	04424	15983	00000
15	78820	00000	96689	66041	66414	02519	01407	96524

Long subtractors

	A	B	C	D	E	F	G	..
		80186		11003		87419	06328	..
1	31892	84351	12991	71381	45306	00473	95127	..
2		74820	22775	74577	16687	00000	02284	..
3			12244	84351	19873	71381	00000	..
4	67072	00473	33541	62771	31360	69320	72030	..
5	45492	77143	26844	74629	53700	02284	00473	..
6	34810	00000	40608	76914	12449	95127	18404	..
7	69256	74272	34948	02284	32231	02255	05262	..
8	23791	61536	49942	96236	37344	00000	08530	..
9	47200	66729	11247	96524	24255	64905	95127	..
10	46921	64905	33541	00000	47580	00473	95127	..
11	24367	96064	02646	03869	02331	64905	95127	..
12	53665	00000	42669	00000	47700	00000	74015	..
13	44882	80277	21048	69320	12780	77848	68166	..
14	75050	18323	07744	19009	18551	68329	00000	..
15	65502	78820	33541	96689	47551	66414	96524	..

Long subtractors

	A	B	C	D	E	F	G	..
		80186		11003		87419	06328	..
1	31892	84351	12991	71381	45306	00473	95127	..
2		74820	22775	74577	16687	00000	02284	..
3			12244	84351	19873	71381	00000	..
4	67072	00473	33541	62771	31360	69320	72030	..
5	45492	77143	26844	74629	53700	02284	00473	..
6	34810	00000	40608	76914	12449	95127	18404	..
7	69256	74272	34948	02284	32231	02255	05262	..
8	23791	61536	49942	96236	37344	00000	08530	..
9	47200	66729	11247	96524	24255	64905	95127	..
10	46921	64905	33541	00000	47580	00473	95127	..
11	24367	96064	02646	03869	02331	64905	95127	..
12	53665	00000	42669	00000	47700	00000	74015	..
13	44882	80277	21048	69320	12780	77848	68166	..
14	75050	18323	07744	19009	18551	68329	00000	..
15	65502	78820	33541	96689	47551	66414	96524	..

Long subtractors

	A	B	C	D	E	F	G	..
	67070	80186	48424	11003	45306	87419	06328	..
1	74820	84351	74577	71381	00000	00473	95127	..
2		74820	84351	74577	71381	00000	02284	..
3			74820	84351	74577	71381	00000	..
4	67072	00473	33541	62771	31360	69320	72030	..
5	45492	77143	26844	74629	53700	02284	00473	..
6	34810	00000	40608	76914	12449	95127	18404	..
7	69256	74272	34948	02284	32231	02255	05262	..
8	23791	61536	49942	96236	37344	00000	08530	..
9	47200	66729	11247	96524	24255	64905	95127	..
10	46921	64905	33541	00000	47580	00473	95127	..
11	24367	96064	02646	03869	02331	64905	95127	..
12	53665	00000	42669	00000	47700	00000	74015	..
13	44882	80277	21048	69320	12780	77848	68166	..
14	75050	18323	07744	19009	18551	68329	00000	..
15	65502	78820	33541	96689	47551	66414	96524	..

Long subtractors