CRT

Display

(HP-41CX, Hewlett Packard 1983 and DM41X, SwissMicros 2020)

Overview[1]

The `CRT` program represents a solution to the Chinese Remainder Theorem which *states that a linear system of congruence equations with pairwise relatively prime moduli has a unique solution modulo the product of the moduli of the system.*

Practically, it goes like this. Imagine a basket of eggs for which it is not known how many there are. Too lazy to count all of them one may know that if you take out three at a time, it ends up with two left-over. If one takes out five at a time, three are left-over, and by taking out seven at a time, two are left-over. This is enough information to figure out the least number of eggs that are in the basket. Here we go.

The basis for finding a solution for an integer number $\mathbf{x}$ which satisfies the congruences of modulo definitions as explained below.

Suppose that $\mathbf{m}_1, \mathbf{m}_2, .., \mathbf{m}_k$ are pairwise relatively prime positive integers, and $\mathbf{a}_1, \mathbf{a}_2, .., \mathbf{a}_k$ is a series of integers, congruences exist as follows:

$\mathbf{x} \equiv \mathbf{a}_i \pmod{\mathbf{m}_i}$ for $i=1..k$ and have a unique solution:

$\mathbf{M} = \mathbf{m}_1 \cdot \mathbf{m}_2 \cdot .. \cdot \mathbf{m}_k$ which is given by:

$\mathbf{x} \equiv \mathbf{a}_1\mathbf{M}_1\mathbf{y}_1 + \mathbf{a}_2\mathbf{M}_2\mathbf{y}_2 + .. + \mathbf{a}_k\mathbf{M}_k\mathbf{y}_k \pmod{\mathbf{M}}$ with:

$\mathbf{M}_i = \mathbf{M}/\mathbf{m}_i$ and $\mathbf{y}_i \equiv 1/\mathbf{M}_i \pmod{\mathbf{m}_i}$ for $i=1..k$

The values $\mathbf{y}_i$ can be found by applying the Extended Euclidean Algorithm.

Example 1

Please note that my default `FIX 5` setting which can be replaced by your preferred number of decimals at line 178. An example is used for the following three congruences:

[1] *This program is copyright and is supplied without representation or warranty of any kind. The author assumes no responsibility and shall have no liability, consequential or otherwise, of any kind arising from the use of this program material or any part thereof*

$$\mathbf{x} \equiv 2 \pmod{3}$$
$$\mathbf{x} \equiv 3 \pmod{5}$$
$$\mathbf{x} \equiv 2 \pmod{7}$$

in which **M**=`LCM(3,5,7)=105` and the value of **x** is to be determined.

KEYSTROKES	DISPLAY	COMMENTS
		Run CRT from the start with: $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$
[XEQ] [ALPHA] CRT [ALPHA]	M 1=?	Enter m_1, which is 3
3 [R/S]	M2=?	Enter m_2, which is 5
5 [R/S]	M3=?	Enter m_3, which is 7
7 [R/S]	M4=?	Press [R/S] to stop more m_i entries
[R/S]	A 1=?	Enter a_1, which is 2
2 [R/S]	A2=?	Enter a_2, which is 3
3 [R/S]	A3=?	Enter a_3, which is 2
2 [R/S]	X=23	Shows x
[USER] [E]	M*= 105	Press User Key E to show M
[USER] [D]	M=(3,5,7)	Press User Key D to show m_1-m_3
[USER] [C]	X=?	Enter a value for X, e.g. 145
145 [R/S]	A=(1,0,5)	Values for a_1-a_3 for same set m_1-m_3
[USER] [B]	A 1=?	Try these reverse values with a_1=1
1 [R/S]	A2=?	Enter a_2=0
0 [R/S]	A3=?	Enter a_3=5
5 [R/S]	X=40	Shows lowest value for x
[USER] [B]	A 1=?	Try these reverse values with a_1=-1
-1 [R/S]	A2=?	Enter a_2=-1
-1 [R/S]	A3=?	Enter a_3=-1
-1 [R/S]	X=40	Shows lowest value for x
[USER] [E]	M*= 105	Shows M
[USER] [A]	M 1=?	Run again by entering new values for m_1-m_k

Example 2

Another example is given with four congruences:

$$\mathbf{x} \equiv 5 \pmod{7}$$
$$\mathbf{x} \equiv 7 \pmod{11}$$
$$\mathbf{x} \equiv 14 \pmod{31}$$
$$\mathbf{x} \equiv 8 \pmod{45}$$

in which **M**=`LCM(7,11,31,45)=107415` and the value of `x` is to be determined.

KEYSTROKES	DISPLAY	COMMENTS
		Run CRT from the start with: $x \equiv 5 \pmod{7} \equiv 7 \pmod{11}$ $x \equiv 14 \pmod{31} \equiv 8 \pmod{45}$
[XEQ][ALPHA]CRT[ALPHA]	M1=?	Enter m_1, which is 7
7[R/S]	M2=?	Enter m_2, which is 11
11[R/S]	M3=?	Enter m_3, which is 31
31[R/S]	M4=?	Enter m_4, which is 45
45[R/S]	M5=?	Press [R/S] to stop more m_i entries
[R/S]	A1=?	Enter a_1, which is 5
5[R/S]	A2=?	Enter a_2, which is 7
7[R/S]	A3=?	Enter a_3, which is 14
14[R/S]	A4=?	Enter a_4, which is 8
8[R/S]	X=20753	Shows x
[USER][E]	M*=107415	Press User Key E to show M=LCM(7,11,31,45)
[USER][D]	M=(7,11,31,45)	Press User Key D to show m_1-m_4
[USER][C]	X=?	Enter a value for X, e.g. 45555
145[R/S]	A=(6,4,16,15)	Values for a_1-a_4 for same set m_1-m_4
[USER][B]	A1=?	Try these reverse values with a_1=6
6[R/S]	A2=?	Enter a_2=4
4[R/S]	A3=?	Enter a_3=16
16[R/S]	A4=?	Enter a_4=15
15[R/S]	X=45555	Shows lowest value for x (same as entry)
[USER][A]	M1=?	Try a new one with m_1=3: $x \equiv 1 \pmod{3} \equiv 6 \pmod{7}$ $x \equiv 10 \pmod{11} \equiv 2 \pmod{13}$ $x \equiv 13 \pmod{17} \equiv 16 \pmod{19}$
3[R/S]	M2=?	Enter m_2=7
7[R/S]	M3=?	Enter m_3=11
11[R/S]	M4=?	Enter m_4=13
13[R/S]	M5=?	Enter m_5=17
17[R/S]	M6=?	Enter m_6=19
19[R/S]	M7=?	Continue to enter values a_i
[R/S]	A1=?	Enter a_1=1
1[R/S]	A2=?	Enter a_2=6
6[R/S]	A3=?	Enter a_3=10
10[R/S]	A4=?	Enter a_4=2
2[R/S]	A5=?	Enter a_5=13
13[R/S]	A6=?	Enter a_6=16
16[R/S]	X=21790	Shows x
[USER][E]	M*=969969	Press User Key E for M=LCM(3,7,11,13,17,19)
[USER][A]	M1=?	Run again by entering new values for m_1-m_k

Program Listing

The listing of CRT is given below with functions A-E in User Mode.

```
01▪LBL "CRT"
02▪LBL A
03 3
04 XEQ 10
05 1
06 ENTER
07▪LBL 02
08 "M"
09 ARCL X
10 >"=?"
11 PROMPT
12 FC?C 22
13 GTO 03
14 STO IND T
15 ST* Z
16 RDN
17 STO 01
18 1
19 ST+ T
20 +
21 GTO 02
22▪LBL 03
23 X<>Y
24 STO 02
25▪LBL B
26 XEQ 10
27 RCL 01
28 3
29 +
30 RCL 01
31 1
32▪LBL 05
33 "A"
34 ARCL X
35 >"=?"
36 PROMPT
37 FC?C 22
38 GTO C
39 STO IND T
40 RDN
41 1
42 ST+ T
43 +
44 X<=Y?
45 GTO 05
46 2
47 R^
48▪LBL 08
49 RDN
50 1
51 ST+ Y
52▪LBL 06
53 STO Z
54 RCL 02
55 *
56 RCL IND Y
57 /
58 LASTX
59 MOD
60 1
61 X=Y?
62 GTO 07
63 X<>Y
64 RDN
65 RCL Z
66 +
67 GTO 06
68▪LBL 07
69 RDN
70 RDN
71 RCL X
72 RCL 01
73 ST+ X
74 +
75 R^
76 STO IND Y
77 2
78 R^
79 STO Z
80 -
81 RCL 01
82 +
83 X>0?
84 GTO 08
85 .
86 STO 00
87 2
88 R^
89▪LBL 09
90 RDN
91 1
92 +
93 RCL 01
94 RCL 02
95 RCL IND Z
96 /
97 RDN
98 +
99 RCL IND X
100 R^
101 *
102 X<>Y
103 RCL 01
104 +
105 RCL IND X
106 X<>Y
107 RDN
108 *
109 ST+ 00
110 RDN
111 STO Y
112 2
113 X<>Y
114 -
115 RCL 01
116 +
117 X>0?
118 GTO 09
119 RCL 00
120 RCL 02
121 MOD
122 "X="
123 ARCL X
124 XEQ 11
125 PROMPT
126 GTO B
127▪LBL C
128 "X=?"
129 PROMPT
130 STO 00
131 XEQ 12
132 "A=("
133 XEQ 10
134▪LBL 00
135 RCL 00
136 RCL IND Y
137 MOD
138 ARCL X
139 >","
140 RDN
141 ISG X
142 GTO 00
143 XEQ 13
144 PROMPT
145 GTO C
146▪LBL D
147 "M=("
148 XEQ 12
149 XEQ 10
150▪LBL 14
151 ARCL IND X
152 RCL 02
153 RCL IND Y
154 ST/ Y
155 MOD
156 X=0?
157 >"*"
158 X<>Y
159 >","
160 ISG X
161 GTO 14
162 XEQ 13
163 PROMPT
164 GTO D
165▪LBL E
166 XEQ 10
167 "M*="
168 ARCL 02
169 XEQ 11
170 PROMPT
171 GTO E
172▪LBL 10
173 CF 29
174 FIX 00
175 RTN
176▪LBL 11
177 SF 29
178 FIX 05
179 RTN
180▪LBL 12
181 RCL 01
182 2
183 +
184 1 E3
185 /
186 3
187 +
188 RTN
189▪LBL 13
190 -1
191 AROT
192 ATOX
193 >")"
194 XEQ 11
195 END
```

(321 bytes)

Registers, Labels and Flags

REGISTERS	COMMENTS
R00	Work solution for x
R01	Number of m_i and a_i, k
R02	LCM(m_1,..,m_k)
R03..R03+k	Values m_1..m_k
R03+k+1..R03+2k	Values a_1..a_k

LABELS	COMMENTS
LBL00	Calculate and show a_i
LBL01	-
LBL02	Entry of m_i
LBL03	Point after entry m_i
LBL04	-
LBL05	Entry of a_i
LBL06	Calculate y_i and M
LBL07	Loop around y_i and M
LBL08	Start of y_i and M loop
LBL09	Calculate x
LBL10	Reset flag and fix number
LBL11	Set flag and fix number
LBL12	Set loop value for m_i and a_i
LBL13	Show m_i and a_i values
LBL14	Show value M
LBL A	User Mode: Entry of all m_i
LBL B	User Mode: Entry of all a_i
LBL C	User Mode: Entry x
LBL D	User Mode: Show all m_i
LBL E	User Mode: Show M

FLAGS	COMMENTS
22	Check for keyboard input
29	Thousands separator

References

Mathematical article: Chinese Remainder Theorem by University of Colorado Denver.
Interactive math website: Chinese Remainder Theorem by *Cut the Knot*.

Downloads

The RAW/TXT format of the program is available via the website: CRT (in zip file).

