

$X=mod(mod(V_1R_1+V_2R_2+V_3R_3+V_4R_4+V_5R_5)M23+T_1R_1+T_2R_2+T_3R_3)MHI+RI$

<i>modulo</i>	2^n	$2^{(n+1)+1}$	$2^{(n+1)-1}$	$2^{(n)+1}$	$2^{(n)-1}$	2^n	$2^{(n+1)+1}$	$2^{(n+1)-1}$					
<i>Modulo value</i>	V_1	V_2	V_3	V_4	V_5	T_1	T_2	T_3	$M23$	$M45$	MHI	C	D
$n=4$	47	139	222	135	221	277	31	33	341	255	86955	5	3
$n=6$	191	1238	3966	2079	715	5205	127	129	5461	4095	21	21	3
$n=8$	6911	17246	60918	33195	12079	8685	511	513	9709	65535	9	9	9
$n=10$	3071	697003	1046526	524799	874325	1394005	2047	2049	1398101	1048575	341	341	3
$n=12$	12287	5584214	16769022	8390655	27982511	22353237	8191	8193	22369621	16777215	1365	1365	3
$n=14$													

<i>modulo</i>	2^n	$2^{(n+1)+1}$	$2^{(n+1)-1}$	$2^{(n)+1}$	$2^{(n)-1}$	2^n	$2^{(n+1)+1}$	$2^{(n+1)-1}$					
<i>Modulo value</i>	V_1	V_2	V_3	V_4	V_5	T_1	T_2	T_3	$M23$	$M45$	MHI		
$n=4$	00101111	10001011	11011110	10000111	11011101	100010101	11111	100001	101010101	11111111	10101001110101011		
$n=6$	000010111111	010011010110	111101111110	100000011111	001011001011	1010001010101	1111111	10000001	1010101010101	11111111111	1010101010011101010101011		
$n=8$	000110101111111	0100001101011110	1110110111110110	1000010001111011	0010111100101111	100001111011101	111111111	1000000001	10010111101101	111111111111111	00100101111011001101101000010011		
$n=10$	0000000010111111111	10101010001010101011	1111111101111111110	10000000000111111111	110101010111101010101	101010100010101010101	11111111111	100000000001	10101010101010101010101	1111111111111111111	10101010101010101001110101010101010101011		
$n=12$	00000000001011111111111	010101010011010101010110	1111111110111111111110	10000000000001111111111	001010101011001010101011	1010101010001010101010101	1111111111111	10000000000001	1010101010101010101010101	11111111111111111111111	101010101010101010100111010101010101010101011		
$n=14$													
<i>Pattern</i>	$V_1=2^{(n+1)+2^{(n)-1}}$ Fazer para n=8,14,20...	Existe padrão (n) n=4, 10,16.. V2=SUM_{i=0,...n} 2^(2i+1)-2^(n+1)+2^(0) n=6, 12,18.. V2=SUM_{i=0,...n} 2^(2i)-2^(n+1)+2^(0) Fazer para n=8,14,20...	$2^{(2n)-2^{(n+1)-2^l}}$ =mod(-2^(n+1)-2^0,2^(2n)-1) V3=-2^(n+1)-1 Fazer para n=8,14,20...	$V_4=2^{(2n-1)+2^{(n-1)-1}}$ Fazer para n=8,14,20...	Existe padrão (n) Similar a V2 (fazer)	Existe Padrão (n) Fazer	T2=2^(n+1)-1	T3=2^(n+1)+1	Existe padrão (n+1) Fazer	M45=2^(2n)-1	Existe Padrão (2n+1) Fazer		

<i>modulo</i>	2^n	$2^{(n+1)+1}$	$2^{(n+1)-1}$	$2^{(n)+1}$	$2^{(n)-1}$	2^n	$2^{(n+1)+1}$	$2^{(n+1)-1}$					
<i>Modulo value</i>	V_1	V_2	V_3	V_4	V_5	T_1	T_2	T_3	$M23$	$M45$	MHI	C	D
$n=3$	23	48	25	56	36	53	15	17	85	63	5355	3	3
$n=5$	287	834	146	217	561	327	63	65	455	1023	465465	4	9
$n=7$	383	16128	5204	2794	8256	21333	255	257	21845	16383	357886635	43	3
$n=9$	1535	261120	173737	218708	131328	347477	1023	1025	349525	262143	91625532075	171	3
$n=11$	12287	5584214	16769022	8390655	27982511	22353237	8191	8193	22369621		1365	1365	3
$n=13$													

<i>modulo</i>	2^n	$2^{(n+1)+1}$	$2^{(n+1)-1}$	$2^{(n)+1}$	$2^{(n)-1}$	2^n	$2^{(n+1)+1}$	$2^{(n+1)-1}$					
<i>Modulo value</i>	V_1	V_2	V_3	V_4	V_5	T_1	T_2	T_3	$M23$	$M45$	MHI		
$n=3$	010111	110000	011001	111000	100100	110101	1111	10001	1010101	111111	1010011101011		
$n=5$	0100011111	1101000010	0010010010	0011011001	1000110001	101000111	111111	1000001	111000111	111111111	01110001101000111001		
$n=7$	00000101111111	11111100000000	01010001010100	00101011101010	10000001000000	101001101010101	11111111	100000001	101010101010101	1111111111111	10101010101001110101010101011		
$n=9$	000000010111111111	111111110000000000	101010011010101001	110101011001010100	100000000100000000	1010100110101010101	1111111111	10000000001	1010101010101010101	11111111111111111	101010101010101010011101010101010101011		
$n=11$	000000010001111111111	1111111101000000000010	1010100111101010100111	1101010110000101010011	1000000000110000000001	111000101000111000111	11111111111	1000000000001	111000111000111000111	111111111111111111111	01110001110001110001101000111000111000111001		
$n=13$													
<i>Pattern</i>	Existe Fazer	Existe Fazer	?	?	Existe Fazer	Existe Padrão (n+1) Fazer	$2^{(n+1)-1}$	$2^{(n+1)+1}$	Existe padrão (n+1) Fazer	$2^{(2n)-1}$	Existe Padrão (2n+1) Fazer		