Solinas primes of small weight for fixed sizes

José de Jesús Angel Angel and Guillermo Morales-Luna
Computer Science Department, CINVESTAV-IPN, Mexico
jjangel@computacion.cs.cinvestav.mx
gmorales@cs.cinvestav.mx

February 2, 2010

Abstract

We give a list of the Solinas prime numbers of the form $f(2^k) = 2^m - 2^n \pm 1$, $m \leq 2000$, with small modular reduction weight $wt < 15$, and $k = 8, 16, 32, 64$, i.e., k is a multiple of the computer integer arithmetic word size. These can be useful in the construction of cryptographic protocols.

1 Introduction

The arithmetic over the primitive prime field $\mathbb{F}_p$ has been used widely in several cryptographic schemes, among them elliptic curve cryptography. Many techniques, implemented both in software and hardware, have been developed to carry out the arithmetic of $\mathbb{F}_p$ in an efficient way [1], [3], [7]. In the same way applications in pairing based cryptography have been used arithmetic over prime fields [5], [7], [8], [10], [11], [12]. Also some other arithmetic procedures over $\mathbb{F}_p$ have been recently proposed in pairing cryptography [6].

Sometimes the form of the prime number determines the arithmetic efficiency, for example a Mersenne prime of the form $p = 2^n - 1$ can change in the modular operation (mod$p$) the integer division by a modular addition. If $p = 2^n - 1$ and it is required to reduce modulo p a $2n$-bit number, usually one proceeds through a division. If $m < p^2$ is the integer number to be reduced modulus p, let us write $m = 2^k A + B$ where A represents the k most significant bits of m. Then $m \equiv (A + B) \bmod p$. The generalization of these numbers was formulated by Solinas in 1999 [13]. A Solinas prime changes the division in the modular operation by a certain number of modular additions and subtractions, called the *modular reduction weight*.

Solinas primes are widely used. For instance, the recommendations on prime fields stated by the NIST consist of Solinas Primes [9]. The NIST primes have been provably efficient in implementations in software and hardware [1] [3] [7]. Some related questions are: how many prime numbers can have small weight?, or is it worth to use other Solinas primes than those selected by NIST?

In this note we count, in the same way as in [2], the prime numbers with small modular reduction weight of the form $2^m \pm 2^n \pm 1$.

This article is organized as follows: In section 2 we recall the definition of the Generalized Mersenne Numbers given by Solinas. In section 3 we display the plots of these numbers. In the appendix we give a list of all the Solinas number primes of the form $2^m - 2^n \pm 1$ with small modular reduction weight, $m \leq 2000$, and $k = 8, 16, 32, 64$, i.e. k is a multiple of the computer integer arithmetic word size.

2 Generalized Mersenne Numbers

Let p be a prime number such that it is represented as the value of an irreducible polynomial, $p = f(t)$, with t being a power of 2, $t = 2^k$. Let $d = \deg(f)$ be the degree of the polynomial $f(X)$. Let us express the powers of t, for exponent greater than $d-1$ within a modular reduction, as

$$\begin{array}{lllllllll} t^d & \equiv & [x_{0,0} & + & x_{0,1}t & + & \cdots & + & x_{0,d-1}t^{d-1}] \mod f(t) \\ t^{d+1} & \equiv & [x_{1,0} & + & x_{1,1}t & + & \cdots & + & x_{1,d-1}t^{d-1}] \mod f(t) \\ \vdots & \vdots & & & & & & & \vdots \\ t^{2d-1} & \equiv & [x_{d-1,0} & + & x_{d-1,1}t & + & \cdots & + & x_{d-1,d-1}t^{d-1}] \mod f(t) \end{array}$$

for integer coefficients x_{ij}. Let

$$M(f) = \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,d-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{d-1,0} & x_{d-1,1} & \cdots & x_{d-1,d-1} \end{pmatrix}.$$

For each column j, let $Y_j = \sum_{\{i| \ x_{i,j}>0\}} x_{i,j}$ be the addition of entries strictly positive and let $Z_j = \sum_{\{i| \ x_{i,j}<0\}} (-x_{i,j})$ be the additive inverse in $\mathbb{Z}$ of the addition of entries strictly negative. Let $Y_M = \max_j Y_j$, and $Z_M = \max_j Z_j$. Let us define the *modular reduction weight* of f as $wt(f) = Y_M + Z_M$.

Remark 1 *The modular reduction weight $wt(f)$ of f is the number of additions and subtractions that replace the division in the* $\bmod\ p$ *operation [13].*

3 Counting Solinas Primes

According to the above discussion, given a multiple m of the word size k it is worth to count the number of cases in which one can have an irreducible polynomial $f(X)$ of degree m/k with smallest possible modular reduction weight such that $p = f(2^k)$ is prime.

The calculation of the map wt is not difficult and it can be done in an efficient way, following the same methods as in [2]. Namely, first, let $p = 2^m \pm 2^n \pm 1$ be a prime

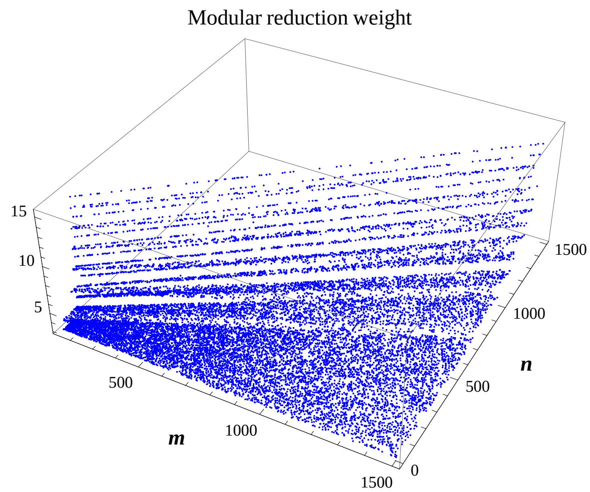

Figure 1: The plot of the modular reduction weight if the polynomial $f(t^k) = 2^m \pm 2^n \pm 1$ is a prime.

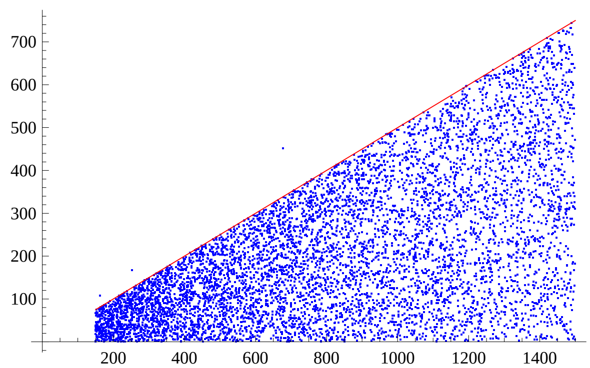

Figure 2: The plot of the m, n with modular reduction weight 3.

number, let $k = \gcd(m, n)$, and let us put $d = m/k$, $c = n/k$ and $f(X) = X^d - X^c \pm 1$. The corresponding matrix M_f and its modular reduction weight wt are obtained immediately. In figure 1 we plot, with respect to the variables m, n, the modular reduction weight corresponding to the polynomial $f(X)$ for $100 \leq m \leq 1500$, and $1 \leq n \leq m$. Let us remark here that within these conditions a small modular reduction weight appears quite often for $n < m/2$. In particular, the parameters m, n producing a polynomial $f(X)$ with weight $wt = 3$ are displayed in figure 2.

The efficiency of the above calculations allows us to find a list of primes p of the form $2^n - 2^m \pm 1$, namely p has n-bits of length, its $wt < 15$, and $64 \leq m \leq 2000$ and $k = 8, 16, 32, 64$.

4 Conclusions

The arithmetic of the prime field $\mathbb{F}_p$ is used in a wide range of cryptographic schemes. Solinas primes, as generalizations of Mersenne primes were standardized as the NIST primes [9]. The list in this paper gives a greater number like those of the NIST and allows to perform efficiently the basic arithmetical operations in the finite fields of the corresponding characteristic.

References

[1] Ananyi K., Rakhmatov D., *Design of a Reconfigurable Processor for NIST Prime Field ECC*, Field-Programmable Custom Computing Machines, 2006. FCCM apos;06. 14th Annual IEEE Symposium on Volume , Issue , 24-26 April 2006 Page(s):333 - 334.

[2] Angel J.J. , Morales G., *Counting Prime Numbers with Short Binary Signed Representation*, Cryptology ePrint Archive: Report 2006/121.

[3] Brown M., Hankerson D., López J., Menezes A., *Software Implementation of the NIST Elliptic Curves Over Prime Fields*, LNCS Volume 2020/2001, Topics in Cryptology, CT-RSA 2001, pp. 250-265.

[4] Chung J.,Hasan A., *More Generalized Mersenne Number*, Report CORR 03-17, University of Waterloo, 2003.

[5] Devegili A. J., Scott M., Dahab R., *Implementing Cryptographic Pairings over Barreto-Naehrig Curves*, Pairing-Based Cryptography, Pairing 2007, LNCS 4575, pp. 197-207.

[6] Fan J.,Vercauteren F., Verbauwhede I. *Faster $\mathbb{F}_p$-Arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves In C* . Clavier, K. Gaj (Eds.), CHES 2009, Lecture Notes in Computer Science, 5747, Springer 2009, p. 240-253

[7] Güneysu T., Paar C., *Ultra High Performance ECC over NIST Primes on Commercial FPGAs*. Cryptographic Hardware and Embedded Systems, CHES 2008, LNCS V. 5154/2008, p. 62-78,

[8] IEEE P1363.3: *Standard for Identity-Based Cryptographic Techniques using Pairings*. http://grouper.ieee.org/groups/1363/IBC/index.html.

[9] National Institute of Standards and Technology (NIST). Federal Information Processing Standard (FIPS) 186-2, *Digital Signature Standard*. 2000.

[10] Request for Comments: 5091, *Identity-Based Cryptography Standard (IBCS) 1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems*, http://www.rfc-editor.org/rfc/rfc5091.txt.

[11] Scott M., *Implementing cryptographic pairings*, Pairing-Based Cryptography, Pairing 2007, Lecture Notes in Computer Science, 4575 (2007), 177-196.

[12] Scott M., *Computing the Tate Pairing*, Topics in Cryptology, CT-RSA 2005, LNCS 3376/2005, pp. 293-304.

[13] Solinas J., *Generalized Mersenne Numbers*, Technical Report CORR 99-39, University of Waterloo, 1999.

ϵ	m	n	d	c	wt	k
$--$	64	8	8	1	3	8
$-+$	64	24	8	3	4	8
$-+$	64	32	2	1	3	32
$-+$	64	40	8	5	6	8
$--$	72	56	9	7	6	8
$--$	80	24	10	3	3	8
$-+$	80	48	5	3	6	16
$-+$	96	32	3	1	4	32
$--$	104	24	13	3	3	8
$--$	112	40	14	5	3	8
$--$	120	88	15	11	5	8
$--$	136	8	17	1	3	8
$--$	136	56	17	7	3	8
$-+$	136	88	17	11	6	8
$--$	136	104	17	13	6	8
$-+$	136	112	17	14	12	8
$--$	144	128	9	8	10	16
$--$	152	24	19	3	3	8
$--$	168	8	21	1	3	8
$-+$	176	48	11	3	4	16
$-+$	176	80	11	5	4	16
$--$	192	16	12	1	3	16
$--$	192	64	3	1	3	64
$-+$	208	24	26	3	4	8
$--$	208	176	13	11	8	16
$-+$	216	152	27	19	8	8
$--$	216	184	27	23	8	8
$-+$	224	96	7	3	4	32
$--$	248	96	31	12	3	8
$--$	248	184	31	23	5	8
$--$	248	200	31	25	7	8
$-+$	256	168	32	21	6	8
$--$	272	40	34	5	3	8

ϵ	m	n	d	c	wt	k
$--$	280	88	35	11	3	8
$-+$	296	80	37	10	4	8
$-+$	296	192	37	24	6	8
$-+$	296	232	37	29	10	8
$-+$	304	184	38	23	6	8
$--$	304	280	38	35	14	8
$--$	312	56	39	7	3	8
$--$	328	184	41	23	4	8
$--$	336	136	42	17	3	8
$--$	336	256	21	16	6	16
$--$	344	120	43	15	3	8
$--$	344	248	43	31	5	8
$-+$	352	120	44	15	4	8
$--$	360	104	45	13	3	8
$-+$	360	272	45	34	10	8
$--$	360	328	45	41	13	8
$-+$	384	80	24	5	4	16
$--$	400	208	25	13	4	16
$--$	400	256	25	16	4	16
$--$	408	128	51	16	3	8
$--$	408	320	51	40	6	8
$--$	416	56	52	7	3	8
$-+$	424	288	53	36	8	8
$-+$	424	296	53	37	8	8
$--$	424	344	53	43	7	8
$--$	432	304	27	19	5	16
$-+$	440	122	55	14	4	8
$--$	464	104	58	13	3	8
$--$	464	264	58	33	4	8
$-+$	498	240	61	30	4	8
$--$	496	8	62	1	3	8
$--$	496	392	62	49	6	8
$-+$	512	32	16	1	4	32

Table 1: A list of all Solinas Prime Numbers, $2^m - 2^n \pm 1$, with small modular reduction weight, and $64 \leq m \leq 512$, where ϵ is the sign sequence.

ϵ	m	n	d	c	wt	k
$--$	512	32	16	1	3	32
$-+$	512	288	16	9	6	32
$-+$	520	424	65	53	12	8
$--$	528	80	33	5	3	16
$-+$	536	56	67	7	4	8
$-+$	544	32	17	1	4	32
$-+$	544	96	17	3	4	32
$-+$	544	184	68	23	4	8
$-+$	544	304	34	19	6	16
$--$	560	192	35	12	3	16
$--$	568	232	71	29	3	8
$-+$	584	376	73	47	6	8
$--$	584	376	73	47	4	8
$--$	600	472	75	59	6	8
$--$	608	72	76	9	3	8
$--$	608	512	19	16	8	32
$-+$	616	216	77	27	4	8
$-+$	624	56	78	7	4	8
$--$	632	96	79	12	3	8
$--$	632	152	79	19	3	8
$--$	632	192	79	24	3	8
$--$	648	64	81	8	3	8
$-+$	648	464	81	58	8	8
$-+$	664	368	83	46	6	8
$-+$	664	560	83	70	14	8
$-+$	688	96	43	6	4	16
$-+$	696	80	87	10	4	8
$--$	696	472	87	59	5	8
$--$	704	56	88	7	3	8
$--$	704	368	44	23	4	16
$-+$	712	88	89	11	4	8
$-+$	712	208	89	26	4	8
$-+$	712	256	89	32	4	8
$--$	744	328	93	41	3	8
$-+$	744	392	93	49	6	8
$-+$	776	256	97	32	4	8

ϵ	m	n	d	c	wt	k
$-+$	784	48	49	3	4	16
$-+$	800	8	100	1	4	8
$--$	816	352	51	22	3	16
$-+$	824	408	103	51	4	8
$-+$	832	72	104	9	4	8
$-+$	832	432	52	27	6	16
$-+$	832	448	13	7	6	64
$--$	840	184	105	23	3	8
$--$	840	496	105	62	4	8
$-+$	856	560	107	70	6	8
$--$	856	728	107	91	8	8
$-+$	864	632	108	79	8	8
$--$	872	264	109	33	3	8
$-+$	880	368	55	23	4	16
$--$	880	448	55	28	4	16
$--$	880	784	55	49	11	16
$--$	896	632	112	79	5	8
$-+$	912	32	57	2	4	16
$--$	912	224	57	14	3	16
$--$	920	152	115	19	3	8
$--$	928	56	116	7	3	8
$-+$	936	512	117	64	6	8
$--$	936	536	117	67	4	8
$--$	936	848	117	106	12	8
$-+$	944	696	118	87	8	8
$-+$	944	784	59	49	12	16
$-+$	952	16	119	2	4	8
$--$	952	352	119	44	3	8
$--$	960	128	15	2	3	64
$-+$	968	296	121	37	4	8
$--$	968	464	121	58	3	8
$--$	976	656	61	41	5	16
$-+$	976	664	122	83	8	8
$--$	976	736	61	46	6	16
$-+$	984	32	123	4	4	8
$-+$	984	680	123	85	8	8

Table 2: A list of all Solinas Prime Numbers, $2^m - 2^n \pm 1$, with small modular reduction weight, and $512 \leq m \leq 984$, where ϵ is the sign sequence.

ϵ	m	n	d	c	wt	k
$-+$	992	408	124	51	4	8
$-+$	992	832	31	26	14	32
$--$	992	912	62	57	14	16
$-+$	1008	776	126	97	10	8
$--$	1024	424	128	53	3	8
$-+$	1024	856	128	107	14	8
$-+$	1032	752	129	94	8	8
$-+$	1040	464	65	29	4	16
$-+$	1040	592	65	37	6	16
$--$	1040	744	130	93	5	8
$-+$	1048	160	131	20	4	8
$--$	1048	296	131	37	3	8
$-+$	1048	528	131	66	6	8
$--$	1056	328	132	41	3	8
$--$	1064	8	133	1	3	8
$-+$	1064	432	133	54	4	8
$--$	1064	520	133	65	3	8
$--$	1088	288	34	9	3	32
$--$	1088	296	136	37	3	8
$-+$	1088	608	34	19	6	32
$--$	1088	896	17	14	7	64
$--$	1096	352	137	44	3	8
$-+$	1096	688	137	86	6	8
$-+$	1104	272	69	17	4	16
$--$	1104	760	138	95	5	8
$--$	1128	320	141	40	3	8
$--$	1128	544	141	68	3	8
$--$	1136	728	142	91	4	8
$-+$	1160	912	145	114	10	8
$--$	1168	296	146	37	3	8
$--$	1176	1048	147	131	11	8
$--$	1184	184	148	23	3	8
$-+$	1184	768	37	24	6	32
$-+$	1192	128	149	16	4	8
$--$	1200	112	75	7	3	16
$--$	1208	24	151	3	3	8
$-+$	1208	288	151	36	4	8
$--$	1208	328	151	41	3	8
$--$	1208	608	151	76	4	8
$-+$	1216	616	152	77	6	8
$-+$	1216	880	76	55	8	16
$--$	1224	464	153	58	3	8
$--$	1232	184	154	23	3	8
$-+$	1232	200	154	25	4	8
$--$	1240	184	155	23	3	8
$--$	1240	712	155	89	4	8
$--$	1256	1144	157	143	13	8
$--$	1264	400	79	25	3	16
$-+$	1264	448	79	28	4	16
$-+$	1272	56	159	7	4	8
$--$	1280	184	160	23	3	8
$--$	1280	496	80	31	3	16
$-+$	1296	248	162	31	4	8
$-+$	1296	896	81	56	8	16
$--$	1296	928	81	58	5	16
$-+$	1304	208	163	26	4	8
$-+$	1304	584	163	73	4	8
$-+$	1312	496	82	31	4	16
$--$	1320	368	165	46	3	8
$-+$	1336	32	167	4	4	8
$--$	1336	632	167	79	3	8
$-+$	1336	696	167	87	6	8
$--$	1336	776	167	97	4	8
$-+$	1336	1048	167	131	10	8
$--$	1344	304	84	19	3	16
$--$	1344	1040	84	65	6	16
$-+$	1352	320	169	40	4	8
$-+$	1352	712	169	89	6	8
$-+$	1360	608	85	38	4	16
$--$	1368	664	171	83	3	8

Table 3: A list of all Solinas Prime Numbers, $2^m - 2^n \pm 1$, with small modular reduction weight, and $992 \leq m \leq 1368$, where ϵ is the sign sequence.

ϵ	m	n	d	c	wt	k
−+	1376	32	43	1	4	32
−+	1376	152	172	19	4	8
−−	1376	664	172	83	3	8
−+	1384	88	173	11	4	8
−+	1384	544	173	68	4	8
−−	1392	904	174	113	4	8
−+	1400	32	175	4	4	8
−−	1400	1192	175	149	8	8
−−	1408	712	176	89	4	8
−−	1424	480	89	30	3	16
−−	1432	232	179	29	3	8
−+	1432	400	179	50	4	8
−−	1440	1304	180	163	12	8
−+	1448	840	181	105	6	8
−−	1472	1264	92	79	9	16
−+	1480	88	185	11	4	8
−−	1480	824	185	103	4	8
−−	1488	272	93	17	3	16
−+	1488	536	186	67	4	8
−−	1496	168	187	21	3	8
−+	1512	32	189	4	4	8
−−	1512	1384	189	173	13	8
−+	1520	544	95	34	4	16
−+	1528	416	191	52	4	8
−−	1528	496	191	62	3	8
−+	1544	248	193	31	4	8
−+	1544	264	193	33	4	8
−+	1544	296	193	37	4	8
−+	1544	904	193	113	6	8
−−	1568	120	196	15	3	8
−+	1576	264	197	33	4	8
−−	1576	872	197	109	4	8
−−	1576	1256	197	157	6	8
−−	1584	896	99	56	4	16
−+	1592	616	199	77	4	8

ϵ	m	n	d	c	wt	k
−−	1592	792	199	99	3	8
−−	1592	1144	199	143	5	8
−+	1600	1272	200	159	10	8
−−	1600	1336	200	167	8	8
−+	1608	80	201	10	4	8
−+	1608	464	201	58	4	8
−+	1608	1136	201	142	8	8
−+	1608	1256	201	157	10	8
−+	1616	1040	101	65	6	16
−+	1624	600	203	75	4	8
−+	1624	688	203	86	4	8
−+	1624	1032	203	129	6	8
−+	1632	200	204	25	4	8
−−	1648	752	103	47	3	16
−+	1656	152	207	19	4	8
−+	1664	840	208	105	6	8
−−	1664	1464	208	183	10	8
−−	1672	640	209	80	3	8
−−	1680	1208	210	151	5	8
−−	1696	632	212	79	3	8
−+	1696	1384	212	173	12	8
−−	1704	1120	213	140	4	8
−−	1712	72	214	9	3	8
−+	1712	1352	214	169	10	8
−+	1720	512	215	64	4	8
−−	1720	664	215	83	3	8
−−	1728	760	216	95	3	8
−−	1728	1328	108	83	6	16
−−	1736	464	217	58	3	8
−+	1744	848	109	63	4	16
−−	1744	1144	218	143	4	8
−+	1776	128	111	8	4	16
−−	1784	224	223	28	3	8
−−	1784	944	223	118	4	8
−−	1792	160	56	5	3	32

Table 4: A list of all Solinas Prime Numbers, $2^m - 2^n \pm 1$, with small modular reduction weight, and $1376 \leq m \leq 1792$, where ϵ is the sign sequence.

ϵ	m	n	d	c	wt	k
$--$	1808	1584	113	99	10	16
$--$	1824	544	57	17	3	32
$-+$	1824	1448	229	181	10	8
$--$	1832	344	229	43	3	8
$-+$	1832	752	229	94	4	8
$-+$	1832	1136	229	142	6	8
$--$	1840	392	230	49	3	8
$--$	1848	128	231	16	3	8
$-+$	1856	1056	58	33	6	32
$--$	1856	1608	232	201	9	8
$-+$	1864	752	233	94	4	8
$-+$	1888	840	236	105	4	8
$-+$	1896	296	237	37	4	8
$-+$	1912	488	239	61	4	8
$-+$	1936	336	121	21	4	16
$--$	1936	712	242	89	3	8
$--$	1944	88	243	11	3	8
$--$	1944	328	243	41	3	8
$--$	1952	1384	244	173	5	8
$-+$	1960	808	245	101	4	8
$-+$	1960	1048	245	131	6	8
$-+$	1968	224	123	14	4	16
$--$	1976	1776	247	222	11	8
$-+$	1984	544	62	17	4	32
$--$	1992	232	249	29	3	8
$--$	2000	1592	250	199	6	8

Table 5: A list of all Solinas Prime Numbers, $2^m - 2^n \pm 1$, with small modular reduction weight, and $1808 \leq m \leq 2000$, where ϵ is the sign sequence.