Counting Prime Numbers with Short Binary Signed Representation

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

Abstract. Modular arithmetic with prime moduli has been crucial in present day cryptography. The primes of Mersenne, Solinas, Crandall and the so called IKE-MODP have been extensively used in efficient implementations. In this paper we study the density of primes with binary signed representation involving a small number of non-zero ± 1-digits.

1. Introduction

Although the prime numbers have been studied along the whole history of science, just after the invention of public key cryptography, prime numbers became essential objects in applied science and they have been the object of intense research. One of the most important tasks concerning prime numbers is modular arithmetic. Prime numbers with few non-zero digits are crucial in the Tate pairing recent implementations.

Some basic problems of modular arithmetic are involved in practical computations, e.g. the problem of reducing modulo n a $2m$-bit number, where m is the bit length of n. This problem can initially be approached by integer division at very high costs [**3**]. Whenever $n = 2^m - 1$ is a Mersenne prime, the division is changed by an addition modulo n [**5**].

Another kind of primes are those of the form $n = 2^m + 1$. It is not difficult to prove that n is a prime if $m = 2^k$, i.e. n is a *Fermat prime*. Nevertheless there are quite few known Fermat primes. A natural way to generalize Mersenne and Fermat primes, was given by Solinas, who proved that for primes whose binary representations involve few signed binary digits, division can be replaced by modular additions and subtractions. The most popular Solinas primes are given in FIPS-186-2 [**4**]:

$$p_{192} = 2^{192} - 2^{64} - 1 \qquad p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$
$$p_{224} = 2^{224} - 2^{96} + 1 \qquad p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$$

Solinas prime p_{224} changes a division by three modular additions, for instance. Also, Crandall [**2**] proposed a new form of primes, namely $n = 2^d - C$, where C is a relatively small odd number, e.g. no longer than the length of a computer word (16-32 bits). When a modulus n is of this form, modular arithmetic can be accomplished using only shifts and additions, eliminating costly divisions. Another kind of prime numbers are the so called *IKE-MODP primes*, which are used in the IKE scheme part of the IPsec protocol. They have the special form $p = 2^n - 2^m + r2^k - 1$, $k < m < n$, r an integer with $0 \leq r < 2^{m-k}$. The number of such primes is estimated directly using Dirichlet's Theorem [**6**].

In this paper we study the density of prime numbers with binary signed representation involving a small number of non-zero ± 1-digits: $2^n \pm 2^{m_k} \pm \cdots \pm 2^{m_1} \pm 1$. This kind of number generalizes the Mersenne, Fermat, Crandall and Solinas primes. Also the above form generalizes the primes considered in [**7**].

In section 2, we introduce some notation for binary signed representations of odd integers and we give simple results of this kind of integers. In section 3 we count in a heuristic way the number of primes of the form $2^n \pm 2^{m_k} \pm \cdots \pm 2^{m_1} \pm 1$, considering $1 \leq k \leq 7$. In section 4 we present some conjectures about the stated heuristic. Finally in section 5 we recall some advantages of these primes.

2. Binary signed expressions

Let $n > 1$ be an integer and let k be another integer such that $1 \leq k < n$. A *formal (n, k)-binary signed expression* has the form:

$$\alpha(\boldsymbol{\varepsilon}, \mathbf{m}) = 2^n + \varepsilon_k 2^{m_k} + \cdots + \varepsilon_1 2^{m_1} + \varepsilon_0 \tag{1}$$

where $1 \leq m_1 < m_2 < \cdots < m_k < n$ and $\boldsymbol{\varepsilon} = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_k) \in \{-1, 1\}^{k+1}$.

Remark 1. *There are $2^{k+1}\binom{n-1}{k}$ different formal (n, k)-binary signed expressions.*

Namely, in eq. (1), there are 2^{k+1} possibilities to choose the sign vector $\boldsymbol{\varepsilon}$ and $\binom{n-1}{k}$ possibilities to choose the vector $\mathbf{m}$ of exponents. Naturally, when interpreted in $\mathbb{Z}$, two different formal (n, k)-binary signed expressions may be equal. Let A_{nk} be the set of positive integers that can be written as (n, k)-binary signed expressions:

$$A_{nk} = \{x \in \mathbb{N} | \exists \boldsymbol{\varepsilon}, \mathbf{m} : \ x = \alpha(\boldsymbol{\varepsilon}, \mathbf{m})\}. \tag{2}$$

Remark 2. *A_{nk} consists just of odd numbers.*

Remark 3. *For each n, k, with $1 \leq k < n$:*

1. *The minimum value of* A_{nk} *is* $m_{nk} = 2^n - \sum_{i=1}^{k} 2^{n-i} - 1$.
2. *The maximum value of* A_{nk} *is* $M_{nk} = 2^n + \sum_{i=1}^{k} 2^{n-i} + 1$.
3. *The mean value of* A_{nk} *is* $\mu_n = \frac{1}{2}(M_{nk} + m_{nk}) = 2^n$
4. A_{nk} *is symmetric with respect to* μ_n*:*
$$x \in A_{nk} \ \& \ |y - \mu_n| = |x - \mu_n| \implies y \in A_{nk}.$$
5. *For any* $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{k-1} \in \{-1, 1\}$
$$2^n - 2^{m_k} + \sum_{i=0}^{k-1} \varepsilon_i 2^{m_i} < \mu_n < 2^n + 2^{m_k} + \sum_{i=0}^{k-1} \varepsilon_i 2^{m_i}$$
($m_0 = 0$*).*

A *Mersenne prime* is any prime of the form $\mu = 2^n - 1$, with $n \in \mathbb{N}$. If we denote by n_i the exponent corresponding to the i-th Mersenne prime μ_i then some examples of Mersenne primes are the following:

i	12	13	14	15	16	17	18
μ_i	$2^{127} - 1$	$2^{521} - 1$	$2^{607} - 1$	$2^{1279} - 1$	$2^{2203} - 1$	$2^{2281} - 1$	$2^{3217} - 1$

Today only 43 Mersenne primes are known, the last one was found on December 15, 2005, and it is $2^{30402457} - 1$. The usual 160-bit modular arithmetic in today's Elliptic Curve Cryptography is within the size of the 13-th Mersenne prime. The *Lenstra-Pomerance-Wagstaff conjecture* states that for any $n \in \mathbb{N}$ the number of Mersenne primes with exponent less than n is asymptotically approximated by the map $n \mapsto e^{\gamma} \log_2(n)$, where $\gamma = \lim_{k \to +\infty} \left(\sum_{\kappa=1}^{k} \frac{1}{\kappa} - \ln(k) \right)$ is the *Euler-Mascheroni constant*.

Solinas primes are generalizations of Mersenne primes [**1**], [**5**]. They are of the form $2^n + \varepsilon_3 2^{m_3} + \varepsilon_2 2^{m_2} + \varepsilon_1 2^{m_1} + \varepsilon_0$, where $\varepsilon_i \in \{-1, +1\}$ and $m_i \equiv 0 \bmod s$ with s being the length of the computer word, e.g. $s = 32$, $0 \leq i \leq 3$ and also $n \equiv 0 \bmod s$. In FIPS-186-2 [**4**] there are introduced the Solinas primes p_{192}, p_{224}, p_{256} and p_{384} as well as the Mersenne prime $p_{521} = 2^{521} - 1$.

The *Crandall primes* are of the form $p = 2^n - C$, where C is an odd number and it is relatively small, for example, no longer than the length of a computer word (16-32 bits).

The main question that we will study is: how many primes possess a formal (n, k)-binary signed expression of the form (1)?

3. Counting primes

First let us consider a number α of the form $2^n + \varepsilon_k 2^{m_k} + \varepsilon_{k-1} 2^{m_{k-1}} + \cdots + \varepsilon_1 2^{m_1} + \varepsilon_0$, being each ε_i a sign ± 1. Let P_{nk} be the set of primes appearing in A_{nk}, $P_{nk} = \{x \in A_{nk} | x \text{ is a prime}\}$. Let a_{nk} be the cardinality of A_{nk}, $a_{nk} = |A_{nk}|$. We look toward an estimation of the cardinality $p_{nk} = |P_{nk}|$. A first approach is to calculate $a_{nk}\Pr(P_{nk}|A_{nk})$ where $\Pr(P_{nk}|A_{nk})$ is the probability that an element in A_{nk} is a prime. According with the Prime Number Theorem, we may expect that $\Pr(P_{nk}|A_{nk}) \approx \frac{2}{n \ln 2}$. Thus, as a first approximation $p_{nk} \approx a_{nk} \frac{2}{n \ln 2}$. Let us observe that:

1. $a_{nk} < 2^{k+1} \binom{n-1}{k}$.
2. $\frac{2}{n \ln 2} < \Pr(P_{nk}|A_{nk})$.
3. If $k \to n-1$, then the interval $[m_{nk}, M_{nk}]$ tends to be $[1, 2^{n+1}]$.
4. If $k \to n-1$, then p_{nk} approaches $\phi(2^{n+1})$ where ϕ is Euler function. Indeed,

$$2^{k+1} \binom{n-1}{k} \frac{2}{n \ln 2} \underset{k \to n-1}{\longrightarrow} 2^n \binom{n-1}{n-1} \frac{2}{n \ln 2} = \frac{2^{n+1}}{\ln(2^n)} \approx \phi(2^{n+1}).$$

Now let us check some particular cases.

3.1. Case $k = 1$. First, let us calculate the number a_{n1} of integers with an expression $2^n + \varepsilon_1 2^{m_1} + \varepsilon_0$, where $n \geq 3$ and $1 \leq m_1 < n$. There are $4 = 2^2$ ways to combine the two signs $\varepsilon_1, \varepsilon_0$. Hence, the number of $(n, 1)$-formal expressions is $2^2(n-1) = 4n-4$. But $2^n + 2 + 1 = 2^n + 2^2 - 1$ and $2^n - 2^2 + 1 = 2^n - 2 - 1$, thus there are $2^2(n-1) - 2 = 4n - 6$ different numbers with a $(n, 1)$-formal expression. Consequently $a_{n1} = 4n - 6$

The greatest number in A_{n1} is $M_{n1} = 2^n + 2^{n-1} + 1$, and the least number is $m_{n1} = 2^n - 2^{n-1} - 1$. From the Prime Number Theorem we have that the probability that an uniformly chosen odd integer in the interval $[m_{n1}, M_{n1}]$ is a prime is $\frac{1}{n} \frac{2}{\ln 2}$. Consequently, a rough estimation for the expectation of p_{n1} is:

$$\lim_{n \to +\infty} \frac{4n-6}{n} \frac{2}{\ln 2} = \frac{8}{\ln 2} \approx 11.541560327111\ldots$$

Using `Mathematica`, for instance, we calculate the number p_{n1} of primes in A_{n1} for some fixed values of n. A graph of all points (n, p_{n1}) for $4 < n < 3500$ is shown in figure 1. Let $P_b = \{p_{n1} | 4 \leq n \leq 3500\}$ be the collection of cardinalities p_{n1} for n in the specified interval. The statistical mean of P_b is $m_{P_b} \approx 14.4$ and its standard deviation is approximately 4.7. The rounding

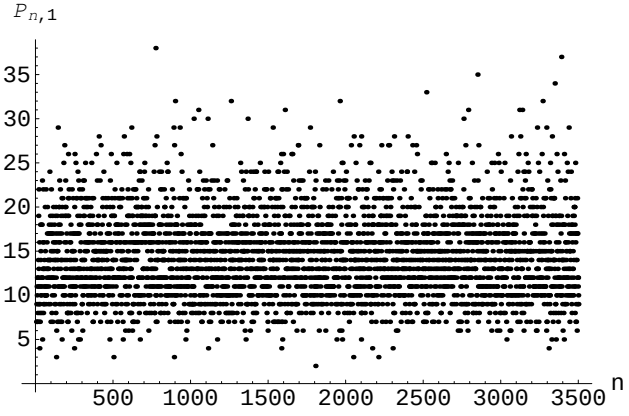

Figure 1: The "ListPlot" of sequence $\{(n, p_{n1})\}_{n\leq 3500}$.

integer of the statistical mean of P_b is 14 as is sketched in figure 1. Thus each $p_{n1} \in P_b$ can be expected to fall in the interval $[14-4, 14+4] = [10, 18]$.

As a second approach, let us observe that the probability to select a prime among the odd integers in the interval $[m_{n1}, M_{n1}]$ can be approximated by $\frac{2}{n\ln(2)}$ and the probability to select a prime in A_{n1}, $\Pr(P_{nk}|A_{nk})$, can be expressed as $\frac{2c_n}{n\ln(2)}$ for a suitable $c_n \in \mathbb{R}$, namely $c_n = \frac{p_{n1}}{2a_{n1}} n\ln 2$. Up to 3500, it can be roughly approximated as $c_{3500} \approx \frac{14.4}{4\cdot 2}\ln(2)$. In figure 2 we plot the points $(n, p_{n1}/a_{n1})$ for $4 \leq n \leq 3500$. The red line corresponds to the map $n \mapsto \frac{2c}{n\ln(2)}$, where $c = 1.24$, and the green line to the map $n \mapsto \frac{2}{n\ln(2)}$. There is no significant difference among them for practical cases.

As an elementary conjecture we may assert: *There exists an increasing sequence of integers* $(n_s)_s$ *such that* $p_{n_s 1} = 0$, $\forall s \in \mathbb{N}$.

In table 1 of appendix A we list the sets $P_{n_s 1}$ for a few integers n_s.

3.2. Case $k = 2$**.** Let us calculate the number a_{n2} of integers having a $(n, 2)$-formal expression $2^n + \varepsilon_2 2^{m_2} + \varepsilon_1 2^{m_1} + \varepsilon_0$, for $n \geq 4$, $1 \leq m_1 < m_2 < n$ and $\varepsilon_2, \varepsilon_1, \varepsilon_0 \in \{-1, +1\}$. The number of these formal expressions is $2^3\binom{n-1}{2} = 4(n-1)(n-2)$. The following equations hold for any $n \geq 4$:

$$\begin{aligned}
2^n + 2^{n-2} - 2 + 1 &= 2^n + 2^{n-1} - 2^{n-2} - 1 \\
2^n + 2^{n-2} + 2 - 1 &= 2^n + 2^{n-1} - 2^{n-2} + 1 \\
2^n + 2^{n-2} + 2 + 1 &= 2^n + 2^{n-2} + 2^2 - 1 \\
2^n + 2^{n-2} + 2^{n-3} - 1 &= 2^n + 2^{n-1} - 2^{n-3} - 1
\end{aligned}$$

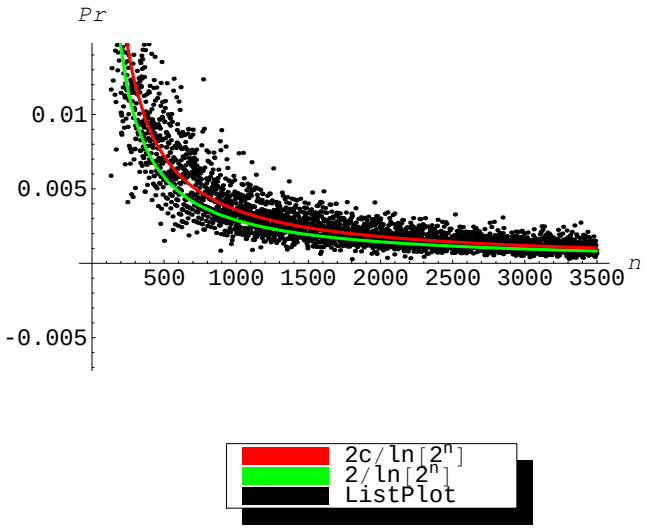

Figure 2: Points $(n, p_{n1}/a_{n1})$ for $4 < n < 3500$ and the maps $n \mapsto \frac{2c_{3500}}{n\ln(2)}$ and $n \mapsto \frac{2}{n\ln(2)}$.

$$\begin{aligned} 2^n + 2^{n-2} + 2^{n-3} + 1 &= 2^n + 2^{n-1} - 2^{n-3} + 1 \\ 2^n + 2^{n-2} - 2^2 + 1 &= 2^n + 2^{n-1} - 2 - 1 \end{aligned}$$

and the corresponding symmetric formulas (according to μ_n) are also valid. Thus, there are 12 numbers repeated in A_{n2}, hence $a_{n2} = 4n^2 - 24n + 46$. Figure 3 plots the points $\{(n, p_{n2}) | 4 \leq n \leq 600\}$. Indeed, they fit to the straight line $p = 10.7935n - 61.6$. By the Prime Number Theorem, the value p_{n2} shall be close to $(4n^2 - 24n + 46)\frac{2}{n\ln(2)}$. As $n \to +\infty$, p_{n2} will tend asymptotically to the straight line $p = 8n\frac{1}{\ln(2)} \approx (11.5416\cdots)n$. In figure 4, we show the "`ListPlot`" of the sequence $\{(n, p_{n2}/a_{n2}) | 4 \leq n \leq 600\}$, and the map $n \mapsto \frac{2}{n\ln(2)}$.

In the current case, the following relations are valid:

1. $p_{n2} = O(n)$.

2. There are around $11 \cdot 160 = 1760$ primes in $A_{160,2}$. A direct calculation shows that actually there are 1520 primes in $A_{160,2}$. Similarly, $11 \cdot 512 = 5632$ is an estimation of the number of primes in $A_{512,2}$. A direct calculation shows that actually there are 6034 primes in $A_{512,2}$.

It is unknown whether *there is an integer n such that A_{n2} contains no primes.* In tables 2 of appendix A we list some sampled primes for some numbers n_s with $k = 2$.

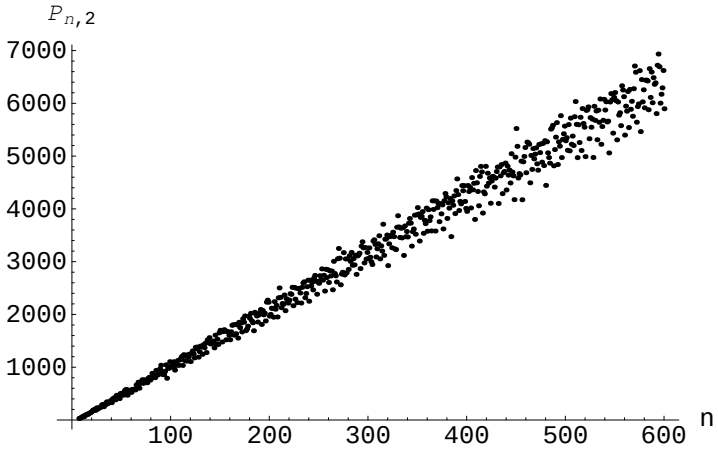

Figure 3: The "ListPlot" of sequence $\{(n, p_{n2})\}_{n\leq 600}$.

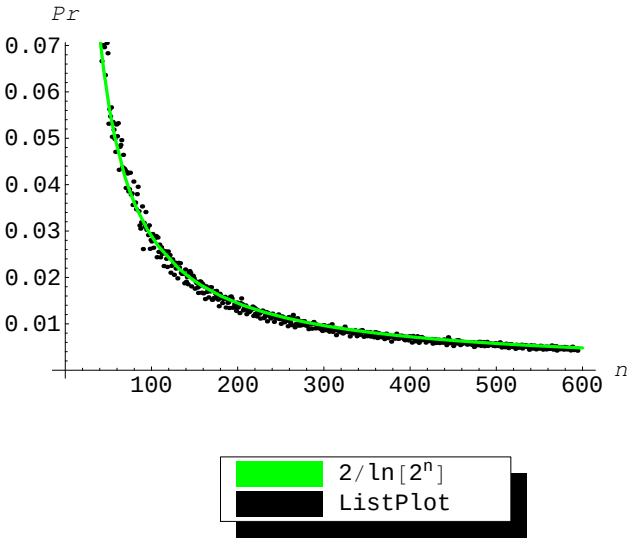

Figure 4: Points $(n, p_{n2}/a_{n2})$ for $4 < n < 600$ and the maps $n \mapsto \frac{2}{n\ln(2)}$

3.3. Cases $k = 3, 4, 5, 6, 7$. For $k = 3, 4, 5, 6, 7$ we have that a_{nk} grows as a polynomial of degree k, $a_{nk} = O(n^k)$. Here we count directly formal (n, k)-binary signed expressions giving the same integer when evaluated, and we get that these numbers r_{nk} have a growth determined by a polynomial of degree $k-1$. An estimation for p_{nk} has a polynomial growth of degree $k-1$, $p_{nk} = O(n^{k-1})$. For the cases of cryptographic interest, they are enough, but the experimental results show that this growth holds for $7 < k < n/2$. Here let us write $f(n) \sim g(n)$ to denote the fact that $\lim_{n\to+\infty} \frac{f(n)}{g(n)} = 1$.

$k = 3$ and $n > 3$.

$$\begin{aligned} a_{n3} &= \frac{8}{3}n^3 - 36n^2 + \frac{544}{3}n - 310 \\ r_{n3} &= 20n^2 - 152n + 294 \\ p_{n3} &\sim (\frac{8}{3}n^3 - 36n^2 + \frac{544}{3}n - 310)\frac{2}{n\ln(2)} \\ &\sim \frac{8}{3}n^3\frac{2}{n\ln(2)} = \frac{16}{3}n^2\frac{1}{\ln(2)} \end{aligned}$$

$k = 4$ and $n > 4$.

$$\begin{aligned} a_{n4} &= \frac{4}{3}n^4 - 32n^3 + \frac{920}{3}n^2 - 1336n + 2222 \\ r_{n4} &= \frac{2}{3}(28n^3 - 390n^2 + 1904n - 3285) \\ p_{n4} &\sim \frac{4}{3}n^4\frac{2}{n\ln(2)} = \frac{8}{3}n^3\frac{1}{\ln(2)} \end{aligned}$$

$k = 5$ and $n > 5$.

$$\begin{aligned} a_{n5} &= \frac{8}{15}n^5 - 20n^4 + 312n^3 - 2480n^2 + 149752n - 16198 \\ r_{n5} &= 12n^4 - \frac{800}{3}n^3 + 2360n^2 - \frac{2244088}{15}n + 16134 \\ p_{n5} &\sim \frac{8}{15}n^5\frac{2}{n\ln(2)} = \frac{16}{15}n^4\frac{1}{\ln(2)} \end{aligned}$$

$k = 6$ and $n > 6$.

$$\begin{aligned} a_{n6} &= \frac{8}{45}n^6 - \frac{48}{5}n^5 + \frac{1996}{9}n^4 - \frac{8320}{3}n^3 + \frac{886592}{45}n^2 \\ &\quad -\frac{1126936}{15}n + 119870 \\ r_{n6} &= \frac{2}{15}(44n^5 - 1430n^4 + 19820n^3 - 145600n^2 + 561116n \\ &\quad -898065) \end{aligned}$$

$$p_{n6} \sim \frac{8}{45}n^6\frac{2}{n\ln(2)} = \frac{16}{45}n^5\frac{1}{\ln(2)}$$

$k = 7$ and $n > 7$.

$$\begin{aligned} a_{n7} &= \frac{16}{315}n^7 - \frac{56}{15}n^6 + \frac{5392}{45}n^5 - \frac{6484}{3}n^4 + \frac{1060912}{45}n^3 \\ &\quad -\frac{2326784}{15}n^2 + \frac{59745032}{105}n - 896406 \\ r_{n7} &= \frac{1}{45}(104n^6 - 4656n^5 + 92780n^4 - 1045440n^3 \\ &\quad +6950336n^2 - 25575144n - 40401405) \\ p_{n7} &\sim \frac{16}{315}n^7\frac{2}{n\ln(2)} = \frac{32}{315}n^6\frac{1}{\ln(2)} \end{aligned}$$

$k > 7$ and $n/2 > k$.

$$p_{nk} \sim \frac{2^{k+1}}{k!}n^k\frac{2}{n\ln(2)} = \frac{2^{k+2}}{k!}n^{k-1}\frac{1}{\ln(2)}$$

In tables 3 of the appendix A we list some sampled prime numbers for some n_s for $k = 3$.

4. Remarks and related questions

In spite of the above mentioned regular behavior of prime numbers in the sets A_{nk}, no conclusive statements can be posed. However, here we dare to pose some intriguing questions about this point.

1. For an increasing sequence of integers $(n_s)_s$ one has $p_{n_s,1} = 0$ for all s.
2. For each $k \geq 2$, there exists an integer $n_k \in \mathbb{N}$ such that $p_{n_k,k} = 0$.
3. There exists an infinity of Solinas' primes.
4. There exists an infinity of Crandall's primes.

5. Advantages in using primes in the sets P_{nk}

With primes in P_{nk}, modular arithmetic is performed more efficiently. In general the primes involving few non-zero digits are used in Miller's method for Tate's pairing evaluation. Also, it is not difficult to find this kind of primes.

The most popular search methods for probable primes have exponential time complexity $O(g^m)$, where m is the probable prime and $g > 1$ is a witness. In the wort case for modular exponentiation, they are required $O(t(m))$ squarings and $wt(m) - 1$ products, where $t(m)$ is the bitlength of m, and $wt(m)$ is the number of $1's$ in its binary representation. For a search method for probable primes, it is possible to precalculate g^{-1}, rendering the same benefits for the signed binary case.

6. Conclusions

In this report we have studied the density of prime numbers involving few non-zero digits in their binary signed expressions. For practical purposes it is not difficult to find such primes and a polynomial estimation can be given of how many such primes are there.

References

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

[2] R.E. Crandall, *Method and apparatus for public key exchange in a cryptographic system*, U.S. Patent # 5,159,632, 1992.

[3] D.E. Knuth, *Seminumerical algorithms*, Addison-Wesley, 1981.

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

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

[6] Yie, I., Lim, S., Kim, S., Kim, D. Prime Numbers of Diffie-Hellman Groups for IKE-MODP, IndoCrypt 2003, *LNCS* 2904. pp. 228-234, 2003.

[7] Wagstaff, S. S. Jr. Prime Numbers with a Fixed Number of One Bits and Zero Bits in Their Binary Representation, *Experimental Mathematics*. 10:2, pp. 267-273, 2000.

A. Listing of some primes in A_{nk}, $k = 1, 2, 3$

In Table 1 we list the primes appearing in sets of the form A_{n1}, for some values of n. Also, in table 2, we list some primes of the form $2^n + \varepsilon_2 2^{m_2} + \varepsilon_1 2^{m_1} + \varepsilon_0$, $(k = 2)$ where $m_1, m_2 \equiv 0 \bmod 16, 32$ respectively and $\varepsilon_i \in \{1, -1\}$. Finally in the tables 3, 4, and 5 we list primes of the form $2^n + \varepsilon_3 2^{m_3} \varepsilon_2 2^{m_2} + \varepsilon_1 2^{m_1} + \varepsilon_0$, $(k = 3)$, where $m_1, m_2, m_3 \equiv 0 \bmod 32$ and $\varepsilon_i \in \{1, -1\}$

$n = 160$	$n = 256$	$n = 320$	$n = 384$	$n = 480$
$2^{160} + 2^3 - 1$	$2^{256} + 2^{96} - 1$	$2^{320} + 2^{22} - 1$	$2^{384} + 2^{33} - 1$	$2^{480} + 2^{385} + 1$
$2^{160} + 2^{110} - 1$	$2^{256} + 2^{106} - 1$	$2^{320} + 2^{36} - 1$	$2^{384} + 2^{301} - 1$	$2^{480} + 2^{92} - 1$
$2^{160} + 2^{117} - 1$	$2^{256} + 2^{130} - 1$	$2^{320} + 2^{159} - 1$	$2^{384} + 2^{341} - 1$	$2^{480} + 2^{122} - 1$
$2^{160} - 2^{31} - 1$	$2^{256} + 2^{166} - 1$	$2^{320} + 2^{190} - 1$	$2^{384} + 2^{343} - 1$	$2^{480} + 2^{211} - 1$
$2^{160} - 2^{76} - 1$	$2^{256} + 2^{196} - 1$	$2^{320} + 2^{196} - 1$	$2^{384} - 2^{60} + 1$	$2^{480} + 2^{274} - 1$
$2^{160} - 2^{86} - 1$	$2^{256} + 2^{203} - 1$	$2^{320} + 2^{232} - 1$	$2^{384} - 2^{80} + 1$	$2^{480} + 2^{318} - 1$
$2^{160} - 2^{91} - 1$	$2^{256} + 2^{206} - 1$	$2^{320} + 2^{286} - 1$	$2^{384} - 2^{218} + 1$	$2^{480} + 2^{371} - 1$
$n = 192$	$2^{256} + 2^{225} - 1$	$2^{320} + 2^{306} - 1$	$2^{384} - 2^{254} + 1$	$2^{480} + 2^{407} - 1$
$2^{192} + 2^9 - 1$	$2^{256} + 2^{231} - 1$	$2^{320} - 2^{92} + 1$	$2^{384} - 2^{306} + 1$	$2^{480} + 2^{463} - 1$
$2^{192} + 2^{19} - 1$	$2^{256} + 2^{252} - 1$	$2^{320} - 2^{164} + 1$	$2^{384} - 2^{125} - 1$	$2^{480} - 2^{140} + 1$
$2^{192} + 2^{20} - 1$	$2^{256} - 2^{168} + 1$	$2^{320} - 2^{194} + 1$	$2^{384} - 2^{185} - 1$	$2^{480} - 2^{374} + 1$
$2^{192} + 2^{41} - 1$	$2^{256} - 2^{174} + 1$	$2^{320} - 2^{270} + 1$	$2^{384} - 2^{186} - 1$	$2^{480} - 2^{129} - 1$
$2^{192} + 2^{65} - 1$	$2^{256} - 2^{76} - 1$	$2^{320} - 2^{288} + 1$	$2^{384} - 2^{254} - 1$	$2^{480} - 2^{168} - 1$
$2^{192} + 2^{86} - 1$	$2^{256} - 2^{194} - 1$	$2^{320} - 2^{308} + 1$	$2^{384} - 2^{293} - 1$	$2^{480} - 2^{185} - 1$
$2^{192} + 2^{120} - 1$	$n = 288$	$2^{320} - 2^{314} + 1$	$2^{384} - 2^{361} - 1$	$2^{480} - 2^{206} - 1$
$2^{192} + 2^{121} - 1$	$2^{288} + 2^7 - 1$	$2^{320} - 2^{105} - 1$	$n = 416$	$2^{480} - 2^{240} - 1$
$2^{192} + 2^{132} - 1$	$2^{288} + 2^{157} - 1$	$2^{320} - 2^{129} - 1$	$2^{416} + 2^{16} - 1$	$2^{480} - 2^{258} - 1$
$2^{192} + 2^{162} - 1$	$2^{288} + 2^{18} - 1$	$2^{320} - 2^{148} - 1$	$2^{416} + 2^{66} - 1$	$2^{480} - 2^{337} - 1$
$2^{192} + 2^{179} - 1$	$2^{288} + 2^{61} - 1$	$2^{320} - 2^{169} - 1$	$2^{416} + 2^{73} - 1$	$2^{480} - 2^{382} - 1$
$2^{192} + 2^{184} - 1$	$2^{288} + 2^{119} - 1$	$2^{320} - 2^{201} - 1$	$2^{416} + 2^{279} - 1$	$2^{480} - 2^{393} - 1$
$2^{192} - 2^{26} + 1$	$2^{288} + 2^{140} - 1$	$2^{320} - 2^{212} - 1$	$2^{416} + 2^{295} - 1$	$2^{480} - 2^{448} - 1$
$2^{192} - 2^{98} + 1$	$2^{288} + 2^{142} - 1$	$2^{320} - 2^{223} - 1$	$2^{416} + 2^{330} - 1$	$2^{480} - 2^{462} - 1$
$2^{192} - 2^{16} - 1$	$2^{288} + 2^{144} - 1$	$2^{320} - 2^{274} - 1$	$2^{416} + 2^{396} - 1$	$2^{480} - 2^{471} - 1$
$2^{192} - 2^{22} - 1$	$2^{288} + 2^{208} - 1$	$2^{320} - 2^{278} - 1$	$2^{416} - 2^{50} + 1$	$n = 512$
$2^{192} - 2^{33} - 1$	$2^{288} + 2^{278} - 1$	$2^{320} - 2^{293} - 1$	$2^{416} - 2^{294} + 1$	$2^{512} + 2^{96} - 1$
$2^{192} - 2^{64} - 1$	$2^{288} - 2^{228} + 1$	$n = 352$	$2^{416} - 2^{356} + 1$	$2^{512} + 2^{124} - 1$
$2^{192} - 2^{67} - 1$	$2^{288} - 2^{246} + 1$	$2^{352} + 2^{97} + 1$	$2^{416} - 2^{410} + 1$	$2^{512} + 2^{190} - 1$
$2^{192} - 2^{127} - 1$	$2^{288} - 2^{276} + 1$	$2^{352} + 2^{44} - 1$	$2^{416} - 2^{56} - 1$	$2^{512} + 2^{490} - 1$
$2^{192} - 2^{164} - 1$	$2^{288} - 2^{36} - 1$	$2^{352} + 2^{89} - 1$	$2^{416} - 2^{98} - 1$	$2^{512} - 2^{32} + 1$
$n = 224$	$2^{288} - 2^{139} - 1$	$2^{352} + 2^{165} - 1$	$2^{416} - 2^{148} - 1$	$2^{512} - 2^{288} + 1$
$2^{224} + 2^{42} - 1$	$2^{288} - 2^{170} - 1$	$2^{352} + 2^{305} - 1$	$2^{416} - 2^{208} - 1$	$2^{512} - 2^{32} - 1$
$2^{224} + 2^{73} - 1$	$2^{288} - 2^{198} - 1$	$2^{352} + 2^{328} - 1$	$2^{416} - 2^{259} - 1$	$2^{512} - 2^{127} - 1$
$2^{224} - 2^6 + 1$	$2^{288} - 2^{199} - 1$	$2^{352} - 2^{42} + 1$	$2^{416} - 2^{321} - 1$	$2^{512} - 2^{190} - 1$
$2^{224} - 2^{20} + 1$	$2^{288} - 2^{230} - 1$	$2^{352} - 2^{70} + 1$	$n = 448$	$2^{512} - 2^{269} - 1$
$2^{224} - 2^{96} + 1$	$2^{288} - 2^{234} - 1$	$2^{352} - 2^{120} + 1$	$2^{448} + 2^{289} - 1$	$2^{512} - 2^{382} - 1$
$2^{224} - 2^{168} + 1$		$2^{352} - 2^{138} + 1$	$2^{448} + 2^{298} - 1$	$2^{512} - 2^{415} - 1$
$2^{224} - 2^{212} + 1$		$2^{352} - 2^{196} + 1$	$2^{448} + 2^{323} - 1$	
$2^{224} - 2^{10} - 1$		$2^{352} - 2^{222} + 1$	$2^{448} + 2^{351} - 1$	
$2^{224} - 2^{23} - 1$		$2^{352} - 2^{246} + 1$	$2^{448} + 2^{382} - 1$	
$2^{224} - 2^{35} - 1$		$2^{352} - 2^{250} + 1$	$2^{448} + 2^{410} - 1$	
$2^{224} - 2^{36} - 1$		$2^{352} - 2^{271} - 1$	$2^{448} + 2^{433} - 1$	
$2^{224} - 2^{118} - 1$		$2^{352} - 2^{103} - 1$	$2^{448} - 2^{220} + 1$	
$2^{224} - 2^{130} - 1$		$2^{352} - 2^{115} - 1$	$2^{448} - 2^{346} + 1$	
$2^{224} - 2^{149} - 1$		$2^{352} - 2^{140} - 1$	$2^{448} - 2^{10} - 1$	
$2^{224} - 2^{154} - 1$		$2^{352} - 2^{167} - 1$	$2^{448} - 2^{224} - 1$	
$2^{224} - 2^{197} - 1$			$2^{448} - 2^{266} - 1$	
			$2^{448} - 2^{358} - 1$	

Table 1: The primes in sets of the form A_{n1}, for some values of n.

ε_2	m_2	ε_1	m_1	ε_0	16	32	ε_2	m_2	ε_1	m_1	ε_0	16	32
$n = 160$													
+1	48	+1	32	+1	√		−1	112	+1	64	+1	√	
+1	128	+1	112	+1	√		−1	112	−1	48	−1	√	
+1	144	−1	112	+1	√								
$n = 192$													
+1	96	+1	48	+1	√		−1	112	+1	32	+1	√	
+1	128	−1	48	+1	√		−1	144	+1	48	+1	√	
+1	144	−1	80	+1	√								
$n = 224$													
+1	128	+1	112	+1	√		−1	192	+1	32	+1	√	√
+1	48	+1	16	−1	√		−1	176	−1	16	−1	√	
+1	208	−1	48	+1	√		−1	176	−1	144	−1	√	
$n = 288$													
+1	192	+1	32	−1	√	√	−1	240	+1	192	+1	√	
+1	128	−1	96	+1	√	√	−1	272	+1	48	+1	√	
+1	224	−1	208	+1	√		−1	224	−1	64	−1	√	√
−1	208	+1	128	+1	√		−1	240	−1	144	−1	√	
$n = 320$													
+1	256	−1	144	+1	√		−1	240	+1	208	+1	√	
+1	288	−1	240	+1	√		−1	288	+1	96	+1	√	√
−1	208	+1	64	+1	√		−1	288	+1	128	+1	√	√
$n = 352$													
+1	224	+1	144	+1	√		+1	336	−1	304	+1	√	
+1	256	+1	176	+1	√		−1	320	−1	160	−1	√	√
+1	288	+1	240	+1	√		−1	336	−1	208	−1	√	
+1	336	+1	192	+1	√								
$n = 384$													
+1	256	+1	208	+1	√		+1	352	+1	128	+1	√	√
+1	288	+1	256	+1	√	√	+1	368	+1	256	+1	√	
+1	64	−1	48	+1	√		+1	272	−1	240	+1	√	√
−1	272	+1	48	+1	√								
$n = 416$													
+1	304	+1	64	+1	√		+1	288	−1	272	+1	√	
+1	352	+1	176	+1	√		+1	336	−1	304	+1	√	
+1	368	+1	320	+1	√		+1	352	−1	320	+1	√	√
+1	384	+1	64	+1	√	√	−1	336	+1	112	+1	√	
+1	288	−1	208	+1	√		−1	400	−1	80	−1	√	
$n = 448$													
+1	64	+1	32	+1	√	√	+1	352	−1	16	+1	√	
+1	240	+1	64	+1	√		−1	368	+1	352	+1	√	
+1	288	+1	208	+1	√		−1	400	+1	256	+1	√	
+1	400	+1	320	+1	√		−1	432	+1	352	+1	√	
+1	400	+1	16	−1	√		−1	160	−1	32	−1	√	√
+1	192	−1	160	+1	√	√							
$n = 480$													
+1	416	+1	208	+1	√		+1	192	−1	176	+1	√	
+1	448	+1	192	+1	√	√	+1	240	−1	80	+1	√	
+1	96	+1	32	−1	√	√	+1	256	−1	160	+1	√	√
+1	272	+1	240	−1	√		+1	368	−1	80	+1	√	
+1	400	+1	304	−1	√								
$n = 512$													
+1	224	+1	64	+1	√	√	+1	352	−1	112	+1	√	
+1	416	+1	384	+1	√	√	+1	416	−1	96	+1	√	√
+1	480	+1	16	+1	√		+1	432	−1	144	+1	√	
+1	480	+1	112	+1	√		−1	288	+1	160	+1	√	√
+1	224	−1	176	+1	√		−1	400	+1	96	+1	√	

Table 2: Some prime numbers of the form $2^n + \varepsilon_2 2^{m_2} + \varepsilon_1 2^{m_1} + \varepsilon_0$, $(k = 2)$, where $m_1, m_2 \equiv 0 \bmod 16$, 32 respectively and $\varepsilon_i \in \{1, -1\}$.

ε_3	m_3	ε_2	m_2	ε_1	m_1	ε_0	ε_3	m_3	ε_2	m_2	ε_1	m_1	ε_0
$n = 192$													
$+1$	96	$+1$	64	-1	32	-1	$+1$	128	-1	96	-1	64	$+1$
$n = 224$													
$+1$	160	-1	64	-1	32	$+1$	-1	192	-1	160	$+1$	64	-1
$n = 256$													
$+1$	96	-1	64	-1	32	-1	-1	224	-1	96	$+1$	64	-1
$n = 288$													
$+1$	224	-1	192	-1	160	$+1$	$+1$	224	-1	64	-1	32	-1
$+1$	256	-1	96	-1	32	-1	$+1$	256	-1	128	-1	32	-1
-1	160	-1	96	$+1$	64	$+1$	-1	192	-1	128	$+1$	64	$+1$
-1	224	-1	128	$+1$	64	-1	-1	192	-1	64	-1	32	$+1$
$n = 320$													
$+1$	128	$+1$	96	-1	32	-1	$+1$	288	-1	192	$+1$	96	-1
$+1$	256	-1	192	-1	32	$+1$	$+1$	224	-1	64	-1	32	-1
$+1$	256	-1	128	-1	32	-1	$+1$	288	-1	128	-1	96	-1
-1	256	$+1$	192	-1	128	-1	-1	224	-1	64	$+1$	32	$+1$
-1	224	-1	192	$+1$	96	$+1$	-1	256	-1	192	$+1$	160	-1
-1	256	-1	160	-1	32	$+1$							
$n = 352$													
$+1$	320	$+1$	256	-1	64	-1	$+1$	320	$+1$	256	-1	160	-1
$+1$	224	-1	160	$+1$	64	-1	$+1$	288	-1	96	$+1$	64	-1
$+1$	320	-1	256	$+1$	96	-1	$+1$	224	-1	160	-1	64	$+1$
$+1$	256	-1	192	-1	96	$+1$	$+1$	256	-1	224	-1	64	$+1$
$+1$	288	-1	256	-1	96	$+1$	$+1$	224	-1	96	-1	64	-1
-1	192	$+1$	160	-1	64	$+1$	-1	320	$+1$	256	-1	32	$+1$
-1	320	$+1$	288	-1	256	$+1$	-1	192	$+1$	128	-1	64	-1
-1	288	$+1$	160	-1	128	-1	-1	320	$+1$	288	-1	128	-1
-1	256	-1	224	$+1$	160	$+1$	-1	320	-1	192	$+1$	32	$+1$
-1	160	-1	128	$+1$	32	-1	-1	288	-1	64	$+1$	32	-1
-1	128	-1	96	-1	64	$+1$	-1	256	-1	160	-1	128	$+1$
-1	320	-1	96	-1	32	$+1$							
$n = 384$													
$+1$	256	$+1$	96	-1	64	-1	$+1$	288	$+1$	192	-1	96	-1
$+1$	352	$+1$	192	-1	128	-1	$+1$	352	$+1$	288	-1	32	-1
$+1$	256	-1	192	$+1$	160	-1	$+1$	288	-1	224	$+1$	32	-1
$+1$	320	-1	256	$+1$	96	-1	$+1$	320	-1	288	-1	128	$+1$
$+1$	352	-1	288	-1	192	$+1$	$+1$	160	-1	128	-1	64	-1
$+1$	256	-1	128	-1	96	-1	$+1$	288	-1	96	-1	64	-1
$+1$	288	-1	128	-1	96	-1	$+1$	320	-1	256	-1	128	-1
-1	352	$+1$	320	-1	160	$+1$	-1	288	$+1$	192	-1	32	-1
-1	320	$+1$	288	-1	96	-1	-1	320	$+1$	288	-1	160	-1
-1	192	-1	160	$+1$	64	$+1$	-1	128	-1	96	$+1$	32	-1
-1	224	-1	160	$+1$	32	-1							

Table 3: Some prime numbers of the form $2^n+\varepsilon_3 2^{m_3}\varepsilon_2 2^{m_2}+\varepsilon_1 2^{m_1}+\varepsilon_0$,$(k = 3)$, where $m_1, m_2, m_3 \equiv 0 \bmod 32$ and $\varepsilon_i \in \{1, -1\}$.

ε_3	m_3	ε_2	m_2	ε_1	m_1	ε_0	ε_3	m_3	ε_2	m_2	ε_1	m_1	ε_0
$n = 416$													
+1	352	+1	192	−1	160	−1	+1	384	+1	256	−1	192	−1
+1	384	+1	320	−1	160	−1	+1	192	−1	160	+1	32	−1
+1	256	−1	128	+1	96	−1	+1	256	−1	192	+1	32	−1
+1	352	−1	256	+1	192	−1	+1	352	−1	320	+1	96	−1
+1	256	−1	64	−1	32	+1	+1	352	−1	64	−1	32	+1
+1	352	−1	224	−1	192	+1	+1	352	−1	288	−1	96	+1
+1	288	−1	192	−1	96	−1	+1	320	−1	128	−1	32	−1
−1	192	+1	128	−1	32	+1	−1	256	+1	192	−1	96	+1
−1	288	+1	256	−1	32	+1	−1	384	+1	288	−1	96	+1
−1	224	+1	96	−1	64	−1	−1	256	+1	160	−1	64	−1
−1	320	+1	288	−1	32	−1	−1	352	+1	320	−1	160	−1
−1	384	−1	352	+1	32	+1	−1	224	−1	160	+1	32	−1
−1	320	−1	128	+1	32	−1	−1	352	−1	256	+1	32	−1
−1	384	−1	224	+1	192	−1	−1	384	−1	288	+1	224	−1
−1	192	−1	128	−1	32	+1	−1	192	−1	128	−1	96	+1
−1	320	−1	96	−1	32	+1	−1	320	−1	256	−1	224	+1
−1	352	−1	288	−1	96	+1	−1	384	−1	256	−1	128	+1
$n = 448$													
+1	224	+1	192	−1	96	−1	+1	320	+1	256	−1	128	−1
+1	384	+1	96	−1	32	−1	+1	384	+1	192	−1	96	−1
+1	384	+1	288	−1	128	−1	+1	384	+1	320	−1	256	−1
+1	352	−1	320	+1	64	−1	+1	384	−1	192	+1	96	−1
+1	384	−1	352	+1	160	−1	+1	320	−1	192	−1	32	+1
+1	384	−1	256	−1	128	+1	+1	416	−1	320	−1	32	+1
+1	416	−1	384	−1	288	+1	+1	320	−1	224	−1	64	−1
+1	352	−1	288	−1	32	−1	+1	352	−1	320	−1	288	−1
+1	416	−1	192	−1	64	−1	+1	416	−1	192	−1	96	−1
+1	416	−1	352	−1	192	+1	+1	416	−1	384	−1	256	−1
−1	288	+1	128	−1	64	+1	−1	320	+1	256	−1	128	+1
−1	320	+1	288	−1	96	+1	−1	384	+1	128	−1	64	+1
−1	384	+1	288	−1	32	+1	−1	416	+1	192	−1	160	+1
−1	320	+1	128	−1	64	−1	−1	352	+1	288	−1	256	−1
−1	256	−1	128	+1	64	+1	−1	288	−1	160	+1	64	+1
−1	288	−1	256	+1	128	+1	−1	352	−1	160	+1	32	+1
−1	384	−1	256	+1	160	+1	−1	416	−1	224	+1	64	+1
−1	416	−1	352	+1	288	+1	−1	320	−1	96	+1	64	−1
−1	416	−1	288	+1	64	−1	−1	224	−1	192	−1	64	+1
−1	384	−1	160	−1	128	+1	−1	384	−1	288	−1	128	+1
−1	384	−1	320	−1	288	+1	−1	384	−1	352	−1	160	+1
−1	416	−1	288	−1	224	+1							
$n = 480$													
+1	288	+1	192	−1	32	−1	+1	320	+1	256	−1	192	−1
+1	352	+1	288	−1	192	−1	+1	384	+1	224	−1	32	−1
+1	384	+1	256	−1	64	−1	+1	416	+1	224	−1	32	−1
+1	416	−1	192	+1	64	−1	+1	448	−1	416	+1	192	−1
+1	288	−1	224	−1	96	+1	+1	320	−1	288	−1	96	+1
+1	448	−1	256	−1	96	+1	+1	224	−1	64	−1	32	+1
+1	384	−1	192	−1	96	−1	+1	416	−1	160	−1	96	−1
+1	448	−1	384	−1	32	−1	−1	352	+1	256	−1	96	+1
−1	384	+1	160	−1	64	+1	−1	288	+1	224	−1	96	−1
−1	320	+1	288	−1	192	−1	−1	352	+1	288	−1	96	−1
−1	384	+1	320	−1	160	−1	−1	384	+1	352	−1	224	−1
−1	416	+1	160	−1	96	−1	−1	448	+1	288	−1	224	−1
−1	352	−1	160	+1	32	+1	−1	224	−1	160	+1	32	−1
−1	256	−1	128	+1	32	−1	−1	288	−1	224	+1	128	−1
−1	416	−1	352	+1	320	−1	−1	448	−1	288	+1	192	−1
−1	448	−1	384	+1	32	−1	−1	448	−1	384	+1	64	−1
−1	288	−1	224	−1	192	+1	−1	352	−1	96	−1	64	+1
−1	352	−1	160	−1	64	+1							

Table 4: Some prime numbers of the form $2^n + \varepsilon_3 2^{m_3} \varepsilon_2 2^{m_2} + \varepsilon_1 2^{m_1} + \varepsilon_0$, $(k = 3)$, where $m_1, m_2, m_3 \equiv 0 \bmod 32$ and $\varepsilon_i \in \{1, -1\}$.

ε_3	m_3	ε_2	m_2	ε_1	m_1	ε_0	ε_3	m_3	ε_2	m_2	ε_1	m_1	ε_0
$n = 512$													
$+1$	320	$+1$	256	-1	128	-1	$+1$	352	$+1$	288	-1	192	-1
$+1$	384	$+1$	320	-1	224	-1	$+1$	448	$+1$	160	-1	32	-1
$+1$	480	$+1$	448	-1	192	-1	$+1$	320	-1	224	$+1$	96	-1
$+1$	416	-1	384	$+1$	160	-1	$+1$	448	-1	224	$+1$	64	-1
$+1$	448	-1	320	$+1$	224	-1	$+1$	480	-1	256	$+1$	160	-1
$+1$	192	-1	128	-1	32	$+1$	$+1$	416	-1	320	-1	224	$+1$
$+1$	448	-1	320	-1	192	$+1$	$+1$	448	-1	352	-1	288	$+1$
$+1$	256	-1	128	-1	64	-1	$+1$	480	-1	224	-1	192	-1
$+1$	480	-1	256	-1	32	-1	$+1$	480	-1	320	-1	192	-1
-1	288	$+1$	160	-1	96	$+1$	-1	320	$+1$	224	-1	192	$+1$
-1	416	$+1$	352	-1	160	$+1$	-1	480	$+1$	160	-1	32	$+1$
-1	480	$+1$	384	-1	192	$+1$	-1	128	$+1$	96	-1	64	-1
-1	160	$+1$	64	-1	32	-1	-1	256	$+1$	192	-1	128	-1
-1	192	-1	160	$+1$	64	$+1$	-1	384	-1	320	$+1$	288	$+1$
-1	416	-1	192	$+1$	96	$+1$	-1	416	-1	352	$+1$	64	$+1$
-1	416	-1	384	$+1$	128	$+1$	-1	416	-1	384	$+1$	160	$+1$
-1	480	-1	384	$+1$	96	$+1$	-1	256	-1	192	$+1$	64	-1
-1	480	-1	320	$+1$	288	-1	-1	288	-1	224	-1	128	$+1$
-1	384	-1	288	-1	192	$+1$	-1	416	-1	384	-1	128	$+1$
-1	448	-1	128	-1	64	$+1$	-1	448	-1	320	-1	96	$+1$
-1	480	-1	224	-1	192	$+1$							

Table 5: Some prime numbers of the form $2^n + \varepsilon_3 2^{m_3} \varepsilon_2 2^{m_2} + \varepsilon_1 2^{m_1} + \varepsilon_0$, $(k = 3)$, where $m_1, m_2, m_3 \equiv 0 \bmod 32$ and $\varepsilon_i \in \{1, -1\}$.