Searching Prime Numbers with Short Binary Signed Representation

Búsqueda de Números Primos con Representaciones Signadas Cortas

José de Jesús Angel Angel[1] and **Guillermo Morales-Luna**[1]

Computer Science Department
CINVESTAV-IPN, Mexico
{jjangel@computacion, gmorales@}cs.cinvestav.mx

Article received on March 1, 2008, accepted on June 14, 2008

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 primes have been widely 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, and its repercussion in the generation of those primes.
Keywords: Pairing cryptography, prime numbers, signed representation.

Resumen
La aritmética de residuos con números primos es crucial en la criptografía actual. Los números primos de Mersenne, Solinas, Crandall y los llamados IKE-MODP han sido extensamente utilizados en diversas implementaciones. Estudiamos aquí la densidad de los primos con representaciones signadas que involucran sólo un número pequeño de dígitos no-nulos ± 1, así como su impacto en la generación de tales primos.
Palabras Claves: Criptografía de emparejamientos, números primos, representaciones signadas.

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 Tate pairing calculation for recent implementations of Pairing Based Cryptography.

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 (Knuth 1997). Whenever $n = 2^m - 1$ is a Mersenne prime, the division is changed by an addition modulo n (Solinas 1999).

Another kind of primes are those of the form $n = 2^m + 1$. It is not difficult to prove that if n is a prime then the exponent has the form $m = 2^k$, 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 ((FIPS) 2000):

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

Solinas prime p_{224} changes a division by three modular additions, for instance. Also, Crandall (Crandall 1994) 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 has this form, modular arithmetic can be accomplished using only shifts and additions, eliminating expensive divisions. Another kind of prime numbers are the so called

IKE-MODP primes (for Internet key exchange based on modular exponentiation), 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 using Dirichlet's Theorem (Yie, Lim, Kim, and Kim 2003).

In this paper we study the density of prime numbers with binary signed representation involving a small number of non-zero ± 1-digits, $2^n + \sum_{j=0}^{k} \varepsilon_j 2^{m_j}$, with $\varepsilon_j \in \{-1, +1\}$, and $m_0 = 0$. This prime numbers generalize the Mersenne, Fermat, Crandall and Solinas primes, as well as the primes considered in (Wagstaff 2000).

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 $2^n + \sum_{j=0}^{k} \varepsilon_j 2^{m_j}$, with $1 \leq k \leq 7$. In section 4 we present some conjectures about the stated heuristic. In section 5 we present the generation and advantages of these primes. Finally in section 6 we recall some of their characteristics.

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:

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

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:

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

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* $m_{nk} = 2^n - \sum_{i=1}^{k} 2^{n-i} - 1 = 2^{n-k} - 1$.
2. *The maximum value of* A_{nk} *is* $M_{nk} = 2^n + \sum_{i=1}^{k} 2^{n-i} + 1 = 2^{n+1} - 2^{n-k} + 1$.
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	$2^{127}-1$	$2^{521}-1$	$2^{607}-1$	$2^{1279}-1$	$2^{2203}-1$	$2^{2281}-1$	$2^{3217}-1$

Up today, only 46 Mersenne primes are known, the last one was found on September, 2008, and it is $2^{32582657}-1$. 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 γ is the *Euler-Mascheroni constant* $\gamma = \lim_{k\to+\infty}\left(\sum_{\kappa=1}^{k}\frac{1}{\kappa} - \ln(k)\right)$.

Solinas primes are generalizations of Mersenne primes (Chung and Hasan 2003), (Solinas 1999). 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. $s = 32$, $0 \le i \le 3$ and also $n \equiv 0 \bmod s$. In FIPS-186-2 ((FIPS) 2000) 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).

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

3 Counting primes

Let a_{nk} be the cardinality of A_{nk}, $a_{nk} = |A_{nk}|$. Let P_{nk} be the set of primes appearing in A_{nk},

$$P_{nk} = \{x \in A_{nk} | x \text{ is a prime}\}.$$

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 to the Prime Number Theorem, $\pi(M_{nk}) \sim \frac{M_{nk}}{\ln(M_{nk})}$ and $\pi(m_{nk}) \sim \frac{m_{nk}}{\ln(m_{nk})}$, where π is Euler's function. We have

$$\begin{aligned}\ln[M_{nk}] &\ge \ln\left[2^{n+1} - 2^{n-k}\right] = \ln\left[2^{n-k}\left(2^{k+1}-1\right)\right] = (n-k)\ln 2 + \ln\left[2^{k+1}-1\right] \ge (n-k)\ln 2 \quad \text{and}\\ \ln[m_{nk}] &\le \ln\left[2^{n-k}\right] = (n-k)\ln 2.\end{aligned}$$

Consequently,

$$p_{nk} \sim \frac{M_{nk}}{\ln(M_{nk})} - \frac{m_{nk}}{\ln(m_{nk})} \le \frac{2}{\ln 2}\frac{2^n - 2^{n-k} + 1}{n-k} = \frac{2}{\ln 2}\frac{M_{nk} - 2^n}{n-k}.$$

Thus, as a rough estimation,

$$\Pr(P_{nk}|A_{nk}) = \frac{p_{nk}}{a_{nk}} \approx \frac{2}{\ln 2}\frac{1}{n-k}\frac{M_{nk}-2^n}{\frac{M_{nk}-m_{nk}}{2}} \approx \frac{2}{(n-k)\ln 2} \approx \frac{2}{n\ln 2}.$$

From here,

$$p_{nk} \approx \frac{2}{n\ln 2} a_{nk}. \tag{3}$$

Let us observe also that:

1. $a_{nk} < 2^{k+1}\binom{n-1}{k}$.
2. $\frac{2}{n\ln 2} < \Pr(P_{nk}|A_{nk})$.
3. As k grows up to $n-1$, then the interval $[m_{nk}, M_{nk}]$ is growing to $[1, 2^{n+1}]$.
4. And as k grows up to $n-1$, the values p_{nk} should approach $\pi(2^{n+1})$.

Now, let us check some particular cases.

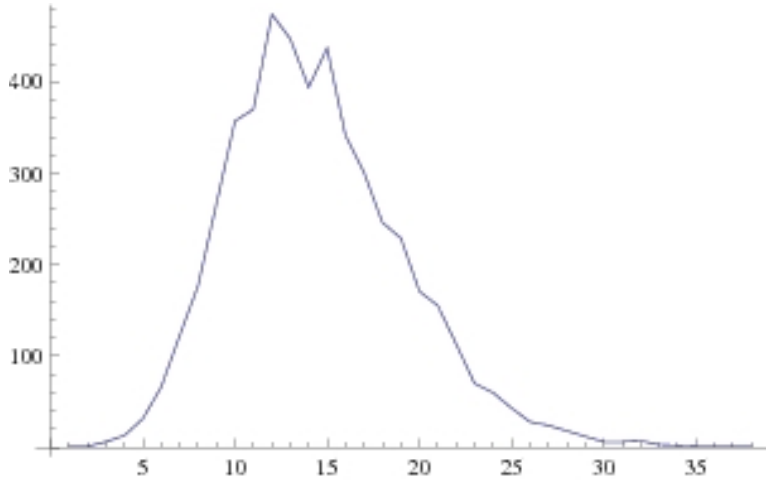


Fig 1. The histogram of values $(p_{n1})_{n\leq 5000}$

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 estimation (3), the expectation of p_{n1} shall be

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

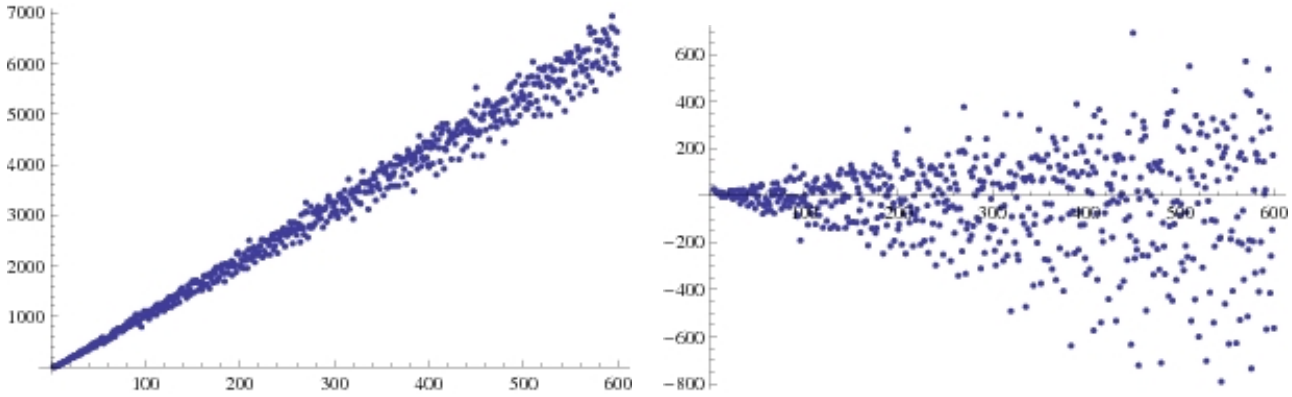
Using `Mathematica`, which in turn uses Miller-Rabin algorithm to test primality, we calculate the number p_{n1} of primes in A_{n1} for $n \leq 5000$. The histogram of the value sequence $P_1 = (p_{n1})_{n\leq 5000}$ is shown in figure 1. For each value p appearing in P_1, it is counted the number c_p of times in which it appears, then the pairs (p, c_p) are joined by straight lines. The most frequent value in P_1, namely the mode of P_1, is 12, the average is $e_1 = 24080/1667 \approx 14.445$ and the standard deviation is $\sigma_1 = \frac{1}{50}\sqrt{\frac{94854953}{1667}} \approx 4.770$. Thus values outside the interval $[e_1 - \sigma_1, e_1 + \sigma_1]$ are scarce. The least value in the examined interval is $p_{1805} = 2$. As an elementary conjecture we may assert: *There exists an increasing sequence of integers* $(n_s)_s$ *such that* $p_{n_s 1} = 2$, $\forall s \in \mathbb{N}$.

For $k = 1$, the horizontal straight line $R_1 :\ p = e_1$ is the best least-squares approximation for $((n, p_{n1}))_{n\leq 5000}$.

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 $n \geq 4$:

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



(a) (b)

Fig 2. (a) The "`ListPlot`" of sequence $P_2 = ((n, p_{n2}))_{3\leq n\leq 600}$. (b) The differences among P_2 and the values given by the straight line R_2

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

for any integer k such that the exponents fall in the interval $[1, n-1]$, 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 2-(a) plots the points $((n, p_{n2}))_{3\leq n\leq 600}$, calculated with Miller-Rabin algorithm and `Mathematica`. Indeed, by least-squares approximation, they fit to the straight line $R_2 :\ p = 10.7924n - 61.164$. According to our estimate (3) we would expect

$$p_{n2} \approx \frac{2}{n \ln 2} a_{n2} = \frac{8}{\ln 2} n - \frac{48}{\ln 2} + \frac{92}{\ln 2} \frac{1}{n} = 11.54n - 69.24 + O(n^{-1}).$$

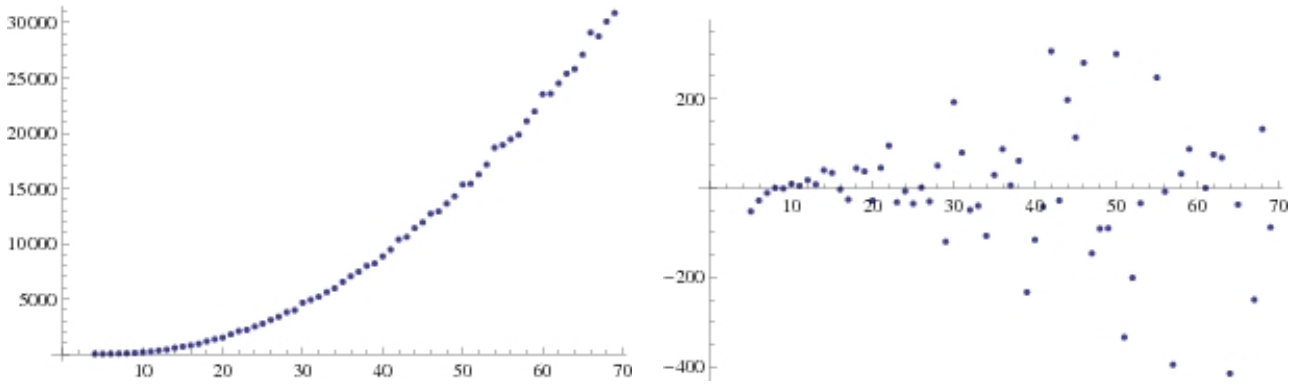
Figure 2-(b) plots the differences among P_2 and the values given by the least square straight line R_2. In this sense, the expected value of p_{n2} behaves as a polynomial of degree 1.

It is not known whether *there is an integer n such that A_{n2} contains no primes*.

3.3 Cases $k = 3, 4, 5, 6, 7$.

For $k = 3, 4, 5, 6, 7$ we have found experimentally that a_{nk} grows as a polynomial of degree k, $a_{nk} = O(n^k)$. Namely, we compute exhaustively the values $(a_{\nu k})_{\nu=k+2}^{2k+2}$ and we interpolate them by a k-degree polynomial $\alpha_k(X) \in \mathbb{Q}[X]$, through canonical Lagrangian procedures. Any further values a_{nk} can be tested to fall as images of the interpolating polynomial, $a_{nk} = \alpha_k(n)$, for each $n \geq k + 2$. Indeed,

$$\begin{aligned} \alpha_3(n) &= \frac{8}{3}n^3 - 36n^2 + \frac{544}{3}n - 310 \\ \alpha_4(n) &= \frac{4}{3}n^4 - 32n^3 + \frac{920}{3}n^2 - 1336n + 2222 \\ \alpha_5(n) &= \frac{8}{15}n^5 - 20n^4 + 312n^3 - 2480n^2 + 149752n - 16198 \\ \alpha_6(n) &= \frac{8}{45}n^6 - \frac{48}{5}n^5 + \frac{1996}{9}n^4 - \frac{8320}{3}n^3 + \frac{886592}{45}n^2 - \frac{1126936}{15}n + 119870 \end{aligned}$$



(a) (b)

Fig 3. (a) The "`ListPlot`" of sequence $P_3 = ((n, p_{n3}))_{4 \leq n \leq 69}$. (b) The differences among P_3 and the values given by the polynomial $\eta_3(n)$

$$\alpha_7(n) = \frac{16}{315}n^7 - \frac{56}{15}n^6 + \frac{5392}{45}n^5 - \frac{6484}{3}n^4 + \frac{1060912}{45}n^3 - \frac{2326784}{15}n^2 + \frac{59745032}{105}n - 896406$$

It is worth to remark at this point that the leading coefficient of polynomial $\alpha_k(X)$ is $\alpha_{kk} = \frac{2^{k+1}}{k!}$.

In fact, if we write $\alpha_k(X) = \sum_{i=0}^{k} \alpha_{ki} X^i$, according to our estimate (3), we expect a number of primes in A_{nk}:

$$p_{nk} \approx \rho_k(n) + O(n^{-1}) = \sum_{i=0}^{k-1} \frac{2\alpha_{k,i+1}}{\ln 2} n^i + O(n^{-1}). \tag{4}$$

The leading coefficient of the $(k-1)$-degree polynomial $\rho_k(X)$ is thus $\rho_{k,k-1} = \frac{2^{k+2}}{k! \ln 2}$.

For instance, for $k = 3$, in figure 3-(a) there is plotted the sequence $P_3 = ((n, p_{n3}))_{4 \leq n \leq 69}$ calculated exhaustively with Miller-Rabin algorithm. The least square quadratic polynomial that fits these values is

$$\eta_3(n) = 7.9163n^2 - 101.511n + 379.246$$

while

$$\rho_3(n) = 7.6943n^2 - 103.874n + 523.217$$

In figure 3-(b) appear the differences, pointwise, among sequence P_3 and the fitting polynomial η_3.

For $k = 4$, in figure 4-(a) there is plotted the sequence $P_4 = ((n, p_{n4}))_{5 \leq n \leq 30}$ calculated exhaustively with Miller-Rabin algorithm. The least square cubic polynomial that fits these values is

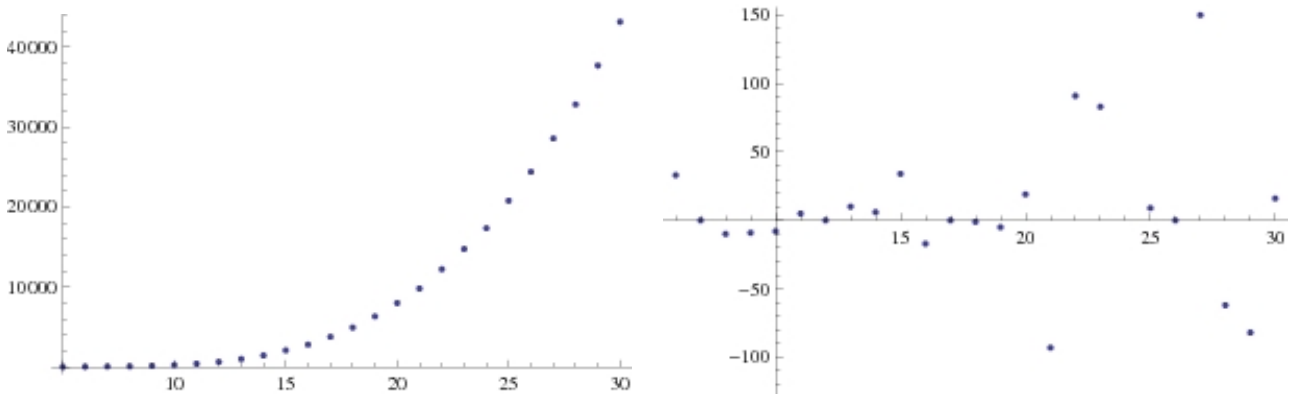
$$\eta_4(n) = 3.5997n^3 - 78.9429n^2 + 620.01n - 1648.94$$

while

$$\rho_4(n) = 3.8471n^3 - 92.3325n^2 + 884.853n - 3854.88$$

In figure 4-(b) appear the differences, pointwise, among sequence P_4 and the fitting polynomial η_4.

For fixed k the exhaustive calculation of p_{nk} requires a_{nk} evaluations of the Miller-Rabin algorithm for numbers of size $n + 1$. Thus, our calculation of p_{nk} has a time complexity $O(n^{k+4})$.



(a) (b)

Fig 4. (a) The "`ListPlot`" of sequence $P_4 = ((n, p_{n4}))_{5 \leq n \leq 30}$. (b) The differences among P_4 and the values given by the polynomial $\eta_4(n)$

4 Remarks and related questions

In spite of the above mentioned "regular behavior" of prime numbers in the sets A_{nk}, i.e.

$$p_{nk} \sim \frac{1}{\ln(2)} \frac{2^{k+2}}{k!} n^{k-1}, \tag{5}$$

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 $p_{n_s,1} = 2$ 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 quantity of Solinas' primes.
4. There exists an infinity quantity of Crandall's primes.

5 Generating Prime Numbers with Short Binary Signed Representation

From the estimation at relation (5), a direct algorithm for finding a prime in P_{nk}, given the parameters n and k, appears plausible: Consecutively choose randomly an odd integer in A_{nk} and stop the first time a prime, witnessed by a primality test, is chosen.

Since, according to (3), $\frac{p_{nk}}{a_{nk}} \sim \frac{2}{\ln(2)} \frac{1}{n}$, the parameter k is mostly irrelevant: In order to find a prime within A_{nk}, the number of attempts tends to coincide with the number of attempts to pick a prime number by random uniform selection within the odd integers of size n, as predicted by the Prime Number Theorem.

In order to obtain primes with short signed binary representations, it is natural to proceed as follows:

Input. n: size of the pretending prime; k: number of signed non-zero digits
Output. p: a prime number of size n with k signed non-zero digits

1. `lead` $= 2^n$; `flag` $=$ `False` ;
2. While `NOT flg` do

(a) choose randomly a k-set $\{m_j\}_{j=1}^{k}$ within the set $\{1,\ldots,n-1\}$. Let $m_0 = 0$;

(b) choose randomly a $(k+1)$-vector of signs $(\varepsilon_j)_{j=0}^{k}$;

(c) let $p = \texttt{lead} + \sum_{j=0}^{k} \varepsilon_j \, 2^{m_j}$;

(d) $\texttt{flag} = \texttt{MillerRabinPrimalityTest}(p)$.

3. Return p.

An experiment of the above algorithm for $n = 163$ in which for each value of k there are generated 50 primes and the number of attempts are averaged to obtain the value μ_{nk}, gives the following results:

k	3	6	9	12	15	18
μ_{nk}	55.58	59.28	52.24	58.54	62.72	54.84

These values are around the expected value $1/(2/(163\ \ln 2)) \approx 56.4915$.
Remark. The expected number of attempts in order to find a prime number of size n, and a given number of non-zero signed digits, is $\lceil \frac{n\ln(2)}{2} \rceil$.

6 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 worst 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.

7 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

Chung, J. and A. Hasan (2003, April). More generalized mersenne number. Technical Report CORR-2003-17, Dept. of Computer Science, University of Waterloo.

Crandall, R. E. (1994). Method and apparatus for public key exchange in a cryptographic system. Technical Report 5463690, U.S. Patents.

(FIPS), F. I. P. S. (2000). Digital signature standard. Technical Report 186-2, National Institute of Standards and Technology (NIST).

Knuth, D. E. (1997, November). *Art of Computer Programming, Volume 2: Seminumerical Algorithms (3rd Edition)*. Addison-Wesley Professional.

Solinas, J. (1999). Generalized Mersenne numbers. Technical Report CORR 1999-39, University of Waterloo.

Wagstaff, S. S. (2000). Prime numbers with a fixed number of one bits and zero bits in their binary representation. *Experimental Mathematics 10*(2), 267–273.

Yie, I., S. Lim, S. Kim, and D. Kim (2003). Prime numbers of diffie-hellman groups for ike-modp. In T. Johansson and S. Maitra (Eds.), *INDOCRYPT*, Volume 2904 of *Lecture Notes in Computer Science*, pp. 228–234. Springer.

José de Jesús Angel-Angel*. received a BSc in Mathematics from National Polytechnic Institute and a MSc degree in Mathematics from Metropolitan Autonomous University, both in Mexico City. At present time is a candidate for a PhD in Computer Science at Cinvestav-IPN. His main interest is in Cryptography. He has attended several congresses and symposia in Canada, South America, Belgium and Spain. He has lectured at the Mexican Military Engineering Academy and other public and private universities in Mexico.*

Guillermo Morales-Luna*. received the BSc degree in mathematics from the Mexican National Polytechnic Institute in 1977, the MSc degree in mathematics from Mexican CINVESTAV-IPN, in 1978, and the Ph.D. degree from the Mathematics Institute of the Polish Academy of Sciences in 1984. Since 1985 he is a researcher at Cinvestav-IPN. His research interest include cryptography, complexity theory, and mathematical logic. He is a Mexican national and he also holds Polish citizenship.*