PU.M.A. Vol. **12** (2001), No. 2, pp. 197-207

Complementary prime-sieve

TAMÁS DÉNES
H-1182. Marosvásárhely u. 13.a.
Budapest, Hungary

(Received: June 10, 2001)

Abstract. The above mentioned "complementary prime-sieve" (for short: C.P.S.) can be characterized as follows:

a necessary sufficient condition is given for natural numbers of forms $6k+1$ and $6k-1$ ($k=1,2,3,...$) when they will be composite numbers.

Theorems 1. and 2. imply a short elementary proof of the infinity of the prime numbers. By C.P.S. does not need the use of Dirichlet's theorem.

With the aid of C.P.S. we are able to generate the prime numbers without factorization and we give an estimate for the cardinality of primes less then X (notation: $\pi(x)$), where X is an arbitrary natural number.

Mathematics Subject Classifications (2000). 11A07, 11A41, 11A51

THEOREM 1 *Every prime number $p>3$ has the forms $6k+1$ or $6k-1$ where $k=1,2,3,\ldots$*

Proof. Let us suppose that p is not of forms $6k+1$ or $6k-1$, this implies:

$$p=6k+2 \quad \text{or} \quad p=6k-2 \tag{1.1}$$

p is an even number, therefore it is a composite number.

$$p=6k+3 \quad \text{or} \quad p=6k-3 \tag{1.2}$$

p is divisible 3, therefore it is a composite number.

$$p=6k+4 \quad \text{or} \quad p=6k-4 \tag{1.3}$$

p is an even number, therefore it is composite number.

$$\begin{array}{l} p=6k+5 \quad \text{or} \quad p=6k-5 \Rightarrow p=6k+5=6(k+1)-1 \quad \text{or} \\ p=6k-5=6(k-1)+1 \end{array} \tag{1.4}$$

these are the forms of the theorem. □

REMARK Dirichlet's theorem states that "If $(a,b)=1$, then the arithmetic progression $ak+b$ ($k=1,2,3,\ldots$) contains infinitely many primes." But our theorem states that every primes are of the forms $6k+1$ or $6k-1$.

According to the Theorem 1. the natural numbers can be ordered in six columns (see Figure 1.), where the first and the fifth column contain all prime numbers (the first column contains of the forms $6k+1$ and the fifth column contains $6k-1$).

$6k+1$				$6k-1$	
↓				↓	
1	2	3	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54
55	56	57	58	**59**	60
61	62	63	64	65	66
67	68	69	70	**71**	72
73	74	75	76	77	78
79	80	81	82	**83**	84
85	86	87	88	**89**	90
91	92	93	94	95	96
97	98	99	100	**101**	102
...					

Figure 1.

Theorem 1. implies a direct upper bound of the cardinality of prime numbers not exceeding N ($\pi(N)$):

$$\pi(N) < \frac{N}{3} \quad \Rightarrow \quad \frac{\pi(N)}{N} < \frac{1}{3} \tag{1.5}$$

As a result of Theorem 1. the determination of prime numbers $p > 3$ makes it possible to enumerate the numbers of the form $6k \pm 1$.

Below (see Theorem 2) we give necessary and sufficient conditions when the numbers of the forms $6k \pm 1$ are composite numbers. These conditions give the procedure, which can be called C.P.S.

THEOREM 2 (COMPLEMENTARY PRIME-SIEVE: C.P.S.) *Let us suppose that N, k, u, v are natural numbers, where $u, v \geq 1$.*

$N = 6k+1$ is a composite number iff $k = 6uv + u + v$ or $k = 6uv - u - v$

$N = 6k-1$ is a composite number iff $k = 6uv - u + v$ or $k = 6uv + u - v$ holds.

Proof of necessity: Let us suppose that $N = 6k+1$ is a composite number, then $6k+1 = dr \Rightarrow k = \frac{dr-1}{6} \Rightarrow dr \equiv 1 \bmod 6$ holds. There are two options:

$$\begin{aligned} &d \equiv 1 \bmod 6 \Rightarrow d = 6u+1 \text{ and } r \equiv 1 \bmod 6 \Rightarrow r = 6v+1 \\ &\Rightarrow k = \tfrac{(6u+1)(6v+1)-1}{6} = \tfrac{36uv+6u+6v+1-1}{6} = 6uv+u+v \end{aligned} \tag{2.1}$$

$$\begin{array}{l} d \equiv -1 \bmod 6 \Rightarrow d = 6u - 1 \text{ and } r \equiv -1 \bmod 6 \Rightarrow r = 6v - 1 \\ \Rightarrow k = \frac{(6u-1)(6v-1)-1}{6} = \frac{36uv-6u-6v+1-1}{6} = 6uv - u - v \end{array} \tag{2.2}$$

If $N = 6k - 1$ is a composite number, then $6k - 1 = dr \Rightarrow k = \frac{dr+1}{6} \Rightarrow dr \equiv -1 \bmod 6$ holds. There are two options:

$$\begin{array}{l} d \equiv 1 \bmod 6 \quad \Rightarrow d = 6u + 1 \text{ and } r \equiv -1 \bmod 6 \quad \Rightarrow r = 6v - 1 \\ \Rightarrow k = \frac{(6u+1)(6v-1)+1}{6} = \frac{36uv-6u+6v-1+1}{6} = 6uv - u + v \end{array} \tag{2.3}$$

This formula (2.3) is symmetric for u, v, so there is another solution:

$$k = 6uv + u - v \tag{2.4}$$

We proved the proof of necessity.

Proof of sufficiency Let us suppose $k = 6uv + u + v$ and $N = 6k + 1$, as well as $v = u + r$, where $u, v \geq 1, r \geq 0$, then

$$\begin{array}{l} N = 6(6u(u+r) + u + u + r) + 1 = 6(6u^2 + 6ur + 2u + r) + 1 \\ = (6u)^2 + 6^2ur + 12u + 6r + 1 \\ = (6u+1)^2 + 6r(6u+1) = (6u+1)(6u+1+6r) = (6u+1)(6v+1) \end{array} \tag{2.5}$$

it is trivially not a prime.

Let us suppose that $k = 6uv - u - v$ and $N = 6k + 1$, as well as $v = u + r$, where $u, v \geq 1, r \geq 0$, then

$$\begin{array}{l} N = 6(6u(u+r) - u - (u+r)) + 1 = 6(6u^2 + 6ur - 2u - r) + 1 \\ = (6u)^2 + 6^2ur - 12u - 6r + 1 \\ = (6u-1)^2 + 6r(6u-1) = (6u-1)(6u-1+6r) = (6u-1)(6v-1) \end{array} \tag{2.6}$$

it is trivially not a prime.

Let us suppose that $k = 6uv - u + v$ and $N = 6k - 1$, as well as $v = u + r$, where $u, v \geq 1, r \geq 0$, then

$$\begin{array}{l} N = 6(6u(u+r) - u + u + r) - 1 = 6(6u^2 + 6ur + r) - 1 \\ = (6u)^2 + 6^2ur + 6r - 1 = (6u+1)(6u-1) + 6r(6u+1) \\ = (6u+1)(6u-1+6r) = (6u+1)(6v-1) \end{array} \tag{2.7}$$

it is trivially not a prime.

Let us suppose that $k = 6uv + u - v$ and $N = 6k - 1$, as well as $v = u + r$, where $u, v \geq 1, r \geq 0$, then

$$\begin{array}{l} N = 6(6u(u+r) + u - (u+r)) - 1 = 6(6u^2 + 6ur - r) - 1 \\ = (6u)^2 + 6^2ur - 6r - 1 = (6u+1)(6u-1) + 6r(6u-1) \\ = (6u-1)(6u+1+6r) = (6u-1)(6v+1) \end{array} \tag{2.8}$$

it is trivially not a prime. □

COROLLARY 3 *As a result of Formulaes* (2.5) – (2.8) *the natural number* $N = 6k \pm 1$ *is represented as a product of* $(6u \pm 1)(6v \pm 1)$.

If $6u-1, 6u+1, 6v-1, 6v+1$ *are prime numbers (by Theorem 1.), then we obtaine prime factorization of* N.

If we induce the notations $a = 6u+1$ *and* $b = 6u-1$, *then all* $N = 6k \pm 1$ *can be represented as one of the following forms* (2.9):

$$N_1 = a(a+6r) \quad N_2 = b(b+6r) \quad N_3 = a(b+6r) \quad N_4 = b(a+6r) \qquad (2.9)$$

EXAMPLE $u = 23, r = 29 \Rightarrow a = 139, b = 137 \Rightarrow$

$N_1 = 139 \times 313 = 43507 \qquad N_2 = 137 \times 311 = 42607$

$N_3 = 139 \times 311 = 43229 \qquad N_4 = 137 \times 313 = 42881.$

COROLLARY 4 *According to that* $a < b$ *always holds and using the notations introduced in Corollary 3* $N_1 \neq N_2 \neq N_3 \neq N_4$ *except when* $r = 0 \Rightarrow N_3 = N_4$.

Checking the magnitudes of N_i *we can obtain the matrix exhibited below (see Figure 2.).*

$$\begin{array}{lll}
N_1 - N_2 = a^2 + 6ar - b^2 - 6br > 0 & \textit{consequently} & N_1 > N_2 \\
N_1 - N_3 = a^2 + 6ar - ab - 6ar > 0 & \textit{consequently} & N_1 > N_3 \\
N_1 - N_4 = a^2 + 6ar - ab - 6br > 0 & \textit{consequently} & N_1 > N_4 \\
N_2 - N_3 = b^2 + 6br - ab - 6ar < 0 & \textit{consequently} & N_2 < N_3 \\
N_2 - N_4 = b^2 + 6br - ab - 6br < 0 & \textit{consequently} & N_2 < N_4 \\
N_3 - N_4 = ab + 6ar - ab - 6br \geq 0 & \textit{consequently} & N_3 \geq N_4
\end{array}$$

	N_1	N_2	N_3	N_4
N_1	–	$>$	$>$	$>$
N_2	$<$	–	$<$	$<$
N_3	$<$	$>$	–	$\geq$
N_4	$<$	$>$	$\leq$	–

Figure 2.

In such a way the relation $N_1 > N_3 \geq N_4 > N_2$ *always holds.*

Theorem 1. and 2. imply a short elementary proof of the infinity of the prime numbers:

COROLLARY 5 *The cardinality of prime numbers are infinite.*

Proof (indirect) Let us suppose that the cardinality of prime numbers are finite.

Theorem 1. is sufficient to investigate natural numbers of the forms $6k \pm 1$.

Let us denote maximal element of prime numbers with $P = 6K + 1$. Consequently all $p > 6K + 1$ natural numbers are composite.

By Theorem 2. (see formulae (2.5), (2.6), (2.7), (2.8)) p factorized into at least two prime factors as follows: $p = \prod_{i=1}^{n} (6u_i \pm 1)(6v_i \pm 1)$ where all $1 \leq i \leq n$ $\Rightarrow 6u_i \pm 1$ and $6v_i \pm 1$ are primes.

The indirect statement implies that all $u_i, v_i < K$, consequently
$p < \prod_{i=1}^{n} (6K \pm 1) < (6K+1)^n$

Thus the cardinality of the natural numbers of form $6k+1$ are finite, but it is not true. Consequently K doesn't exist, thus the indirect statement is false.

The use of form $6k+1$ is enough to complete the proof, but we could follow the same way with the use of $6k-1$. □

COROLLARY 6 *By formulae* (2.5) – (2.8) *we are investigating the cardinality of composite numbers of forms* $6k+1$ *and* $6k-1$ *up to* N. *It means that we are investigating the inequality* $N_i \leq N \quad (i = 1,2,3,4)$.

$$N_1 \leq N \Rightarrow (6u+1)(6u+1+6r) \leq N \Rightarrow r \leq \frac{N}{6(6u+1)} - \frac{6u+1}{6} = \frac{N-(6u+1)^2}{6(6u+1)} \xrightarrow{v=u+r(def.)} \tag{2.10}$$

$$v \leq \frac{N-(6u+1)^2}{6(6u+1)} + u \Rightarrow v \leq \frac{N-6u-1}{6(6u+1)} \tag{2.11}$$

$$N_2 \leq N \Rightarrow (6u-1)(6u-1+6r) \leq N \Rightarrow r \leq \frac{N}{6(6u-1)} - \frac{6u-1}{6} = \frac{N-(6u-1)^2}{6(6u-1)} \xrightarrow{v=u+r(def.)} \tag{2.12}$$

$$v \leq \frac{N-(6u-1)^2}{6(6u-1)} + u \Rightarrow v \leq \frac{N+6u-1}{6(6u-1)} \tag{2.13}$$

$$N_3 \leq N \Rightarrow (6u+1)(6u-1+6r) \leq N \Rightarrow r \leq \frac{N}{6(6u+1)} - \frac{6u-1}{6} = \frac{N-(6u)^2+1}{6(6u+1)} \xrightarrow{v=u+r(def.)} \tag{2.14}$$

$$v \leq \frac{N-(6u)^2+1}{6(6u+1)} + u \Rightarrow v \leq \frac{N+6u+1}{6(6u+1)} \tag{2.15}$$

$$N_4 \leq N \Rightarrow (6u-1)(6u+1+6r) \leq N \Rightarrow r \leq \frac{N}{6(6u-1)} - \frac{6u+1}{6} = \frac{N-(6u)^2+1}{6(6u-1)} \xrightarrow{v=u+r(def.)} \tag{2.16}$$

$$v \leq \frac{N-(6u)^2+1}{6(6u-1)} + u \Rightarrow v \leq \frac{N-6u+1}{6(6u-1)} \tag{2.17}$$

By formulae N_i $(i = 1,2,3,4)$, *the pair* u, v *is symmetrical. Clearly in case of* $u \neq v$ *for* $r > 0$ *the values of* N_i *determine all composite numbers of form* $6k+1$ *and* $6k-1$. *That implies the formulae below:*

$$r = 0 \Rightarrow N_1 = (6u+1)^2 \quad \textit{consequently } N_1 \leq N \Rightarrow (6u+1)^2 \leq N \Rightarrow u \leq \frac{\sqrt{N}-1}{6} \tag{2.18}$$

$$r = 0 \Rightarrow N_2 = (6u-1)^2 \quad \textit{consequently } N_2 \leq N \Rightarrow (6u-1)^2 \leq N \Rightarrow u \leq \frac{\sqrt{N}+1}{6} \tag{2.19}$$

$$r \Longrightarrow N_3 = N_4 = (6u)^2 - 1 \quad \textit{consequently } N_3, N_4 \leq N \Rightarrow (6u)^2 - 1 \leq N \Rightarrow u \leq \frac{\sqrt{N+1}}{6} \tag{2.20}$$

Let us introduce the notation $K_i(N)$, that will denote the number of composite numbers for which $N_i \leq N$ holds.

$$K_1(N) = \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N-6u-1}{6(6u+1)} - u + 1\right) \tag{2.21}$$

$$K_2(N) = \sum_{u=1}^{\frac{\sqrt{N}+1}{6}} \left(\frac{N+6u-1}{6(6u-1)} - u + 1\right) \tag{2.22}$$

$$K_3(N) = \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N+6u+1}{6(6u+1)} - u + 1\right) \tag{2.23}$$

$$K_4(N) = \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N-6u+1}{6(6u-1)} - u + 1\right) \tag{2.24}$$

$$K(N) = K_1(N) + K_2(N) + K_3(N) + K_4(N) \tag{2.25}$$

The proof mentioned above ensured the necessity only i.e. producing all different pairs u, v.

That makes the occurrence of the composite number possible more than once. Let us denote the number of composite numbers up to N with $K\pi(N)$. $m(N)$ denotes the composite numbers' occurrence more than once.

$$K\pi(N) = K(N) - m(N) \tag{2.26}$$

Let us denote with $KP(N)$ the number of prime numbers obtained with the aid of C.P.S.:

$$KP(N) = \left[\frac{N}{3}\right] - K\pi(N) \tag{2.27}$$

If we know the exact value of $m(N)$ that implies the formulae (2.28):

$$\pi(N) = \left[\frac{N}{3}\right] - K\pi(N) = KP(N) \tag{2.28}$$

COROLLARY 7 *Formulae (2.21)–(2.25) imply an approximation of $K(N)$. Easy to see that formula (2.29) holds.*

$$\left|(\sqrt{N} \pm 1) - \sqrt{N}\right| = 1 \quad \text{as well as} \quad \sqrt{N+1} - \sqrt{N} < 1 \tag{2.29}$$

Without losing the generality the formulae (2.21) – (2.24) we can use the value $\frac{\sqrt{N}}{6}$ to sum:

$$\begin{aligned} K(N) \;=\; & \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\tfrac{N-6u-1}{6(6u+1)} + \tfrac{N+6u-1}{6(6u-1)} + \tfrac{N+6u+1}{6(6u+1)}\right. \\ & \left. + \tfrac{N-6u+1}{6(6u-1)} - 4u + 4\right) \end{aligned} \tag{2.30}$$

If $a = 6u+1$ *and* $b = 6u-1 \Rightarrow K(N)$

$$\begin{aligned}
&= \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\tfrac{N-a}{6a} + \tfrac{N+b}{6b} + \tfrac{N+a}{6a} + \tfrac{N-b}{6b} - 4u + 4\right) \\
&= \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\tfrac{2N}{6a} + \tfrac{2N}{6b} - 4u + 4\right) = \tfrac{2N}{6} \sum_{u=1}^{\frac{\sqrt{N}}{6}} \tfrac{a+b}{ab} - \tfrac{4(1+\frac{\sqrt{N}}{6})\frac{\sqrt{N}}{6}}{2} + \tfrac{4\sqrt{N}}{6} \qquad (2.31) \\
&= \tfrac{2N}{6} \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\tfrac{12u}{36u^2-1}\right) - \tfrac{4\sqrt{N}}{6}\left(\tfrac{6+\sqrt{N}}{12} - 1\right) \\
&= 4N \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\tfrac{u}{36u^2-1}\right) - \tfrac{N}{18} + \tfrac{\sqrt{N}}{3}
\end{aligned}$$

Easy to see that $36u^2 - 1 \approx 36u^2 \quad \Rightarrow \frac{u}{36u^2-1} \approx \frac{u}{36u^2} = \frac{1}{36u}$, *in such a way for* $K(N)$ *the result is the following:*

$$K(N) \approx 4N \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\frac{1}{36u}\right) - \frac{N}{18} + \frac{\sqrt{N}}{3} = \frac{\sqrt{N}}{3} - \frac{N}{18} + \frac{N}{9} \sum_{u=1}^{\frac{\sqrt{N}}{6}} \frac{1}{u} \qquad (2.32)$$

The approximation of $\sum \frac{1}{u}$ *inequalities might be used* (2.33) *(see* [5]*):*

$$1 + \log(n) \geq \sum_{u=1}^{n} \frac{1}{u} > \log(n+1) \qquad (2.33)$$

We obtained as below (2.34)*:*

$$\frac{N}{18} + \frac{\sqrt{N}}{3} + \frac{N}{9}\log\left(\frac{\sqrt{N}}{6}\right) \geq K(N) > \frac{\sqrt{N}}{3} - \frac{N}{18} + \frac{N}{9}\log\left(\frac{\sqrt{N}}{6} + 1\right) \qquad (2.34)$$

Let us suppose that mean of (2.34) *left and right side is the approximation of* $K(N)$ *(denote:* $KK(N)$*).*

$$K(N) \approx KK(N) = \frac{\sqrt{N}}{3} + \frac{N}{18}\log\frac{N+6\sqrt{N}}{36} \qquad \xrightarrow{(2.26),\,(2.27)} \qquad (2.35)$$

$$\begin{aligned}
KP(N) &\approx \left[\tfrac{N}{3}\right] - KK(N) + m(N) \\
&= \left[\tfrac{N}{3}\right] - \tfrac{\sqrt{N}}{3} - \tfrac{N}{18}\left(\tfrac{\log N}{2} + \log(\sqrt{N}+6) - \log 36\right) + m(N)
\end{aligned}$$

COROLLARY 8 *Similarly to formulae* (2.10) – (2.17) *we shall investigate the inequalities* $N_i \geq M \quad (i = 1,2,3,4)$ *where* $M < N$ *is a natural number.*

$$N_1 \geq M \Rightarrow \quad v \geq \frac{M - 6u - 1}{6(6u+1)} \qquad (2.36)$$

$$N_2 \geq M \Rightarrow v \geq \frac{N + 6u - 1}{6(6u-1)} \qquad (2.37)$$

$$N_3 \geq M \Rightarrow v \geq \frac{N + 6u + 1}{6(6u+1)} \qquad (2.38)$$

$$N_4 \geq M \Rightarrow v \geq \frac{N-6u+1}{6(6u-1)} \tag{2.39}$$

Obviously the above mentioned formulae is defined in the interval (M,N). *Let us introduce the notation* $K_i(M,N)$ $(i=1,2,3,4)$ *that will denote the number of pairs* (u,v) *composite numbers included in the interval* (M,N)*:*

$$\begin{aligned} K_1(M,N) &= \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N-6u-1}{6(6u+1)} - \frac{M-6u-1}{6(6u+1)} + 1\right) \\ &= \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N-M}{6(6u+1)} + 1\right) \end{aligned} \tag{2.40}$$

$$\begin{aligned} K_2(M,N) &= \sum_{u=1}^{\frac{\sqrt{N}+1}{6}} \left(\frac{N+6u-1}{6(6u-1)} - \frac{M+6u-1}{6(6u-1)} + 1\right) \\ &= \sum_{u=1}^{\frac{\sqrt{N}+1}{6}} \left(\frac{N-M}{6(6u-1)} + 1\right) \end{aligned} \tag{2.41}$$

$$\begin{aligned} K_3(M,N) &= \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N+6u+1}{6(6u+1)} - \frac{M+6u+1}{6(6u+1)} + 1\right) \\ &= \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N-M}{6(6u+1)} + 1\right) \end{aligned} \tag{2.42}$$

$$\begin{aligned} K_4(M,N) &= \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N-6u+1}{6(6u-1)} - \frac{M-6u+1}{6(6u-1)} + 1\right) \\ &= \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N-M}{6(6u-1)} + 1\right) \end{aligned} \tag{2.43}$$

$$K(M,N) = K_1(M,N) + K_2(M,N) + K_3(M,N) + K_4(M,N) \tag{2.44}$$

Below we give the equivalent formulae for (2.26), (2.27), (2.32), (2.35) in arbitrary interval (M,N).

$$K\pi(M,N) = K(M,N) - m(M,N) \tag{2.45}$$

$$KP(M,N) = \left[\frac{N-M}{3}\right] - K\pi(M,N) \tag{2.46}$$

$$\begin{aligned} K(M,N) &= \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\frac{N-M}{6(6u+1)} + \frac{N-M}{6(6u-1)} + \frac{N-M}{6(6u+1)} + \frac{N-M}{6(6u-1)} + 4\right) \\ &= 4(N-M) \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\frac{u}{36u^2-1}\right) + \frac{2\sqrt{N}}{3} \end{aligned} \tag{2.47}$$

$$36u^2 - 1 \approx 36u^2 \Rightarrow \frac{u}{36u^2 - 1} \approx \frac{u}{36u^2} = \frac{1}{36u},$$

thus we give for $K(M,N)$*:*

$$K(M,N) \approx 4(N-M)\sum_{u=1}^{\frac{\sqrt{N}}{6}}(\frac{1}{36u}) + \frac{2\sqrt{N}}{3} = \frac{2\sqrt{N}}{3} + \frac{N-M}{9}\sum_{u=1}^{\frac{\sqrt{N}}{6}}\frac{1}{u} \quad (2.48)$$

For the approximation of $\sum \frac{1}{u}$ *we can apply the mean value of formulae* (2.33)*:*

$$KK(M,N) = \frac{2\sqrt{N}}{3} + \frac{N-M}{18}(1 + \log\frac{N+6\sqrt{N}}{36}) \quad (2.49)$$

If $N = 6k+1$ *or* $N = 6k-1$ *is a composite number, then two factorable representation of* N *by* (2.49) *maximum steps are needed:*

$$N = M \overset{(2.49)}{\longrightarrow} KK(M,N) = \frac{2\sqrt{N}}{3} \quad (2.50)$$

C.P.S. gives a direct representation of composite numbers in an interval (M,N)*. Consequently one can obtain the prime numbers of interval* (M,N)*.*

By that approach one can obtain efficient methods to solve three basic tasks about the prime numbers:

1. Given an interval (M,N)*. Enumerate all prime numbers from that interval.*

2. Let us represent the prime numbers up to N*. (Then* $M = 1$*)*

3. Decide whether a natural number p *is a prime itself.*

In RSA (Rivest, Shamir, Adleman) cryptosystem the tasks 1–3 might be used with practical values. In a forthcoming paper we shall hopefully return to that applications.

OPEN PROBLEMS AND CONJECTURES: What is an exact value of $m(N)$? or What is a good approximate of $m(N)$? These questions are equivalent the following problem:

Let us the following equalities

— $k_1 = v(6u+1) + u$ — $k_2 = v(6u-1) - u$

— $k_3 = v(6u-1) + u$ — $k_4 = v(6u+1) - u$

If $1 \leq u,v \leq C$ (C is an arbitrary natural number) and $i \neq j$, then how many times are there $k_i = k_j$?

CONJECTURE 1.: $KP(N)$ approximates $\pi(N)$.

CONJECTURE 2.: The relative error of $KP(N)$ and $\pi(N)$ better than $\pi N)$ and $\frac{N}{\log N}$.

Figure 3. demonstrates the paper's results on the cardinality of prime numbers.

N	$K(N)$	$KK(N)$	$m(N)$	$KP(N)$	$\pi(N)$	$\frac{N}{\log(N)}$	$KP(N)$ *rel.err.*	$\frac{N}{\log(N)}$ *rel.err.*
1000	205	195	34	162	168	144	3.5%	14.3%
2000	484	461	112	294	303	263	3.0%	13.2%
3000	794	755	214	420	430	375	2.3%	12.8%
4000	1118	1067	325	540	552	482	2.2%	12.7%
5000	1452	1394	442	656	669	587	2.0%	12.3%
6000	1807	1731	577	770	783	690	1.7%	11.8%
7000	2160	2077	713	886	900	791	1.5%	12.1%
8000	2532	2431	857	991	1007	890	1.5%	11.6%
9000	2905	2792	1006	1101	1117	988	1.4%	11.5%
10000	3281	3159	1160	1212	1229	1086	1.4%	11.6%
11000	3666	3531	1316	1316	1335	1182	1.4%	11.5%
12000	4055	3909	1474	1419	1438	1278	1.3%	11.1%
13000	4454	4291	1648	1527	1547	1372	1.3%	11.3%
14000	4850	4677	1815	1631	1652	1466	1.2%	11.3%
30000	11641	11266	4891	3250	3245	2910	0.2%	10.3%
50000	20796	20175	9263	5133	5133	4621	0.0%	10.0%
70000	30409	29537	14013	6937	6935	6275	0.0%	9.5%
90000	40335	39220	19053	8718	8713	7890	0.0%	9.4%
190000	92971	90619	46813	17175	17170	15632	0.0%	8.9%
350000	183080	178739	96357	29943	29977	27417	0.1%	8.5%
900000	517786	506647	289266	71480	71274	65645	0.1%	7.9%
1000000	581158	568777	326493	78668	78498	72382	0.2%	7.8%
1500000	905437	886863	520366	114929	114155	105478	0.6%	7.6%
2000000	1239132	1214375	721684	149218	148933	137849	0.2%	7.4%
3000000	1926146	1889011	1143113	216967	216818	201152	0.6%	7.2%
4000000	2632033	2582508	1581846	283146	283148	263127	0.0%	7.0%
5000000	3351917	3290031	2033930	348679	348515	324150	0.4%	7.0%
6000000	4083022	4008733	2495735	412713	412851	384436	0.3%	6.9%
7000000	4823413	4736732	2966794	476714	476650	444122	0.1%	6.8%
8000000	5571739	5472690	3445726	540653	539779	503304	0.1%	6.7%
10000000	7088528	6964708	4416529	661334	664579	620421	0.4%	6.6%

Figure 3.

Acknowledgment

I am happy to thank Dr S.W. Golomb for the informative letter (see [1]) in which he explained that he has published the theorem "A necessary and sufficient condition that there be infinitely many twin primes is that there be infinitely many numbers n not of the form $6ab \pm a \pm b$." and he wrote up-to-date historical background to it. It gives the inspiration to my next paper on the twin prime problem based on C.P.S.

Many thanks to my father Dr József Dénes for his useful help in the preparation of this paper.

References

[1] T. DÉNES, *New results in RSA key description* (in Hungarian), Híradástechnika, **1** (2002), 47–55.

[2] T. DÉNES, *Complementary Prime Sieve and a remark on S.W. Golomb's factorization method* (manuscript).

[3] S.W. GOLOMB, FAX massage to J.Dénes (dated 21.07.2000.) *Problem E969*, American Math. Monthly, **58** (1951), no.5. 338.

[4] S.W. GOLOMB, *On factoring Jevons' number*, CRYPTOLOGIA, **XX** (1996), No3.

[5] P. ERDŐS, J. SURÁNYI: *Selected chapters from the theory of numbers*, (in Hungarian) Polygon, Szeged, 1996.

[6] MARIA SUZUKI, *Alternative formulations of the twin prime problem*, The Amer. Math. Monthly, **107** (2000).