Complementary prime-sieve
and
a remark on S.W. Golomb’s factorization method

Tamás Dénes **Budapest, Hungary**

October, 2001.

ABSTRACT

The above mentioned *"complementary prime-sieve"* (for short: *C.P.S.*) can be characterize as follows:
Our Theorem 1. is, every prime number *(greater then 3)* has the forms *6k-1* or *6k+1 (k= natural number).* After it, *we are given a necessary sufficient condition for 6k+1 and 6k-1 (k=1,2,3,...,natural number) in which a composite number*. C.P.S. does not seek for a prime number (as other sieves do), but sieves the composite numbers which left are prime numbers (therefore this will call a complementery prime-sieve). By C.P.S. does not need the use of Dirichlet's theorem. With aid C.P.S. we are able to generate the prime numbers without factorization and at the same time we give a new method for factorization of composite numbers.
With C.P.S. we makes better the factorization method of S.W. Golomb, which appered in CRYPTOLOGIA, vol. XX. Number 3. as "On factoring Jevons’ number".

Theorem 1.

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

Proof:

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

(1.1) p= 6k+2 or p= 6k-2 *p* is even number, therefore it is composite number.

(1.2) p= 6k+3 or p= 6k-3 *p* is divisible 3, therefore it is composite number.

(1.3) p= 6k+4 vagy p= 6k-4 *p* is even number, therefore it is composite number.

(1.4) p= 6k+5 vagy p= 6k-5 $\Rightarrow$ p= 6k+5 = 6(k+1)-1 or p= 6k-5 = 6(k-1)+1
these are the form of theorem.

Q.E.D.

Remark:

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

By Theorem 1. the natural numbers ordered in six column (see Figure 1.), then all prime numbers contain column first and fifth column (first contains 6k+1 and column fifth contains 6k-1).

Figure 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**
. . . .					

By Theorem 1. implies the "fast" upper bound of the number of prime numbers less or equal to N (denote: $\pi(N)$):

(1.5) $$\pi(N) \langle \frac{N}{3} \Rightarrow \frac{\pi(N)}{N} \langle \frac{1}{3}$$

By Theorem 1. the determination of prime numbers $p\rangle 3$ makes it possible to enumerate of the form $6k\pm1$.
Below (see Theorem 2.) we give necessery and sufficient conditions when the numbers is the form $6k\pm1$ composite numbers. These conditions give the method and procedure, which can be called to C.P.S.

Theorem 2. (Complementary Prime-Sieve: C.P.S.)

Let us suppose that N, k, u, v be natural numbers, where $u,v \geq 1$.
N= 6k+1 a composite number iff $k = 6uv + u + v$ *or* $k = 6uv - u - v$
N= 6k -1 a composite number iff $k = 6uv - u + v$ *or* $k = 6uv + u - v$ *holds.*

Proof of necessity:

Let us suppose $N = 6k+1$ 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:

(2.1) $d \equiv 1 \bmod 6 \Rightarrow$ **d= 6u+1 and** $r \equiv 1 \bmod 6 \Rightarrow$ **r= 6v+1**

$$\Rightarrow \mathbf{k} = \frac{(6u+1)(6v+1)-1}{6} = \frac{36uv+6u+6v+1-1}{6} = \mathbf{6uv + u + v}$$

(2.2) $d \equiv -1 \bmod 6 \Rightarrow$ **d= 6u-1 and** $r \equiv -1 \bmod 6 \Rightarrow$ **r= 6v-1**

$$\Rightarrow \mathbf{k} = \frac{(6u-1)(6v-1)-1}{6} = \frac{36uv-6u-6v+1-1}{6} = \mathbf{6uv - u - v}$$

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

There are two options:

(2.3) $d \equiv 1 \bmod 6 \Rightarrow$ **d= 6u+1 and** $r \equiv -1 \bmod 6 \Rightarrow$ **r= 6v-1**

$$\Rightarrow \mathbf{k} = \frac{(6u+1)(6v-1)+1}{6} = \frac{36uv-6u+6v-1+1}{6} = \mathbf{6uv - u + v}$$

For this formula (2.3) is symmetric for u, v, so there is another solution holds:

(2.4) $k = 6uv + u - v$

We proved the necessity of the proof.

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

(2.5) $N=6(6u(u+r)+u+u+r)+1 = 6(6u^2+6ur+2u+r)+1 = (6u)^2+6^2ur+12u+6r+1=$
$=(6u+1)^2+6r(6u+1)=(6u+1)(6u+1+6r)=$ $(6u+1)(6v+1)$
it is trivially not a prime.

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

(2.6) $N=6(6u(u+r)-u-(u+r))+1 = 6(6u^2+6ur-2u-r)+1 = (6u)^2+6^2ur-12u-6r+1=$
$=(6u-1)^2+6r(6u-1)=(6u-1)(6u-1+6r)=$ $(6u-1)(6v-1)$ *it is trivially not a prime.*

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

(2.7) $N=6(6u(u+r)-u+u+r)-1 = 6(6u^2+6ur+r)-1 = (6u)^2+6^2ur+6r-1=$
$=(6u+1)(6u-1)+6r(6u+1) = (6u+1)(6u-1+6r) = (6u+1)(6v-1)$
it is trivially not a prime.

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

(2.8) $N=6(6u(u+r)+u-(u+r))-1 = 6(6u^2+6ur-r)-1 = (6u)^2+6^2ur-6r-1=$
$=(6u+1)(6u-1)+6r(6u-1) = (6u-1)(6u+1+6r) = (6u-1)(6v+1)$
it is trivially not a prime.

Q.E.D.

Corollary 2.1.

Formulae (2.5) - (2.8) gave the natural number $N= 6k \pm 1$ represented as a product of $(6u \pm 1)(6v \pm 1)$.
If *6u-1, 6u+1, 6v-1, 6v+1* are prime numbers (as it is possible by Theorem 1.), then we obtained prime factorization of *N*.

We induced the notations $a=6u+1$ and $b=6u-1$, then all $N=6k \pm 1$ can be represented in one of the form to (2.9) form:

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

Example:
u=23, r=29 $\Rightarrow$ a=139, b=137 $\Rightarrow$ N_1= 139x313= 43507 N_2= 137x311= 42607
N_3= 139x311= 43229 N_4= 137x313= 42881

Now we apply the C.P.S. to make better the factorization method of S.W. Golomb (see [1]). Golomb’s method inspired by W.S Jevons’ problem, which published in his book in the 1873’ (see [2]). Jevons in this book presented a specific ten-digit number (8.616.460.799) whose prime factorization, he believed, would forever remain unknown except to himself. *The prime factorization method of S.W. Golomb:*
Let us p and q arbitrary prime numbers and their product is J. We can write:

(3.1) $$J = p \cdot q = a^2 - b^2 = (a+b)(a-b)$$

where a and b are natural numbers.

We set $a_0 = \left[\sqrt{J}\right]$ and let $a_k = a_0 + k$ for k=1,2,3,...
We look successively at $a_k^{\,2} - J$ to see if any of these is a perfect square, thus

(3.2) $$a_k^{\,2} - J = b_k^{\,2} \Rightarrow J = (a_k + b_k)(a_k - b_k)$$

We apply the Golomb method for the Jevons’ number, that specifically J=8.616.460.799 *k=56* , a_{56}=92.880, b_{56}=3199.

$$(a_{56}^{\,2} - b_{56}^{\,2} = (a_{56} - b_{56})(a_{56} + b_{56}) = \underbrace{89681}_{p} \cdot \underbrace{96079}_{q} = 8.616.460.799 = J)$$

The other way by the C.P.S. we give a factorization of J to two prime factors, like the form (3.3):

(3.3) $$J = (6u \pm 1)(6v \mp 1) \qquad (u, v = 1,2,3, \ldots)$$

If we consider the equations (3.2) and (3.3) that imply

(3.4) $$J = (a_k + b_k)(a_k - b_k) = (6u \pm 1)(6v \mp 1)$$

From the condition of J is product of two primes and the (3.3), (3.4) equations follows the next states

(3.5) if $J=6K+1$, then $a_k + b_k = 6u \pm 1$ and $a_k - b_k = 6v \pm 1$
if $J=6K-1$, then $a_k + b_k = 6u \pm 1$ and $a_k - b_k = 6v \mp 1$

And the addition of two equations imply:

(3.6) $$2a_k = 6u + 6v \pm 2 \Rightarrow a_k = 3(u+v) \pm 1$$
$$2a_k = 6u + 6v \Rightarrow a_k = 3(u+v)$$

From (3.6) follows the state that a_k , or $a_k \pm 1$ divides by 3, thus we set the a_0 as it appears from (3.7)

(3.7) $$h \equiv \left[\sqrt{J}\right] \bmod 3 \quad \Rightarrow \quad a_0 = \left[\sqrt{J}\right] - h$$

namely a_0 divides by 3, then from the Golomb's method implies that *k* divides by 3 too, or $k \equiv \pm 1 \bmod 3$:

(3.8) $$a_k = a_0 + k$$

That is, we pay attantion to only the steps *k=3,6,9, ...* , or *k=1,4,7,..., or k=2,5,8,...* of success are sufficient. Applied this result on the Jevons' number:

(3.9) $$a_0 \xrightarrow{(8)} 92823 \qquad (h=1)$$
$$a_{19\cdot 3} = 92880$$

Consequently that *k=19* steps of algorithm *(instead of k=56)* would have been sufficient!

Finally remarkable that the C.P.S. gives a direct representation of composite number in an interval (M,N). Consequently one can obtain the prime numbers of interval (M,N). By that approach one obtained efficient methods to solve three basic tasks about the prime numbers:
1. Given an interval (M,N) enumerate all possible prime numbers from that interval.
2. Let us represent the prime numbers up to N. (Then M=1)
3. Decide a natural number p prime itself ?

An RSA (Rivest, Shamir, Adleman) encipherment system the task 1.-3. might used with a practical values. The real possibility which increase the effectiveness of C.P.S. is the parallel computation.

------------------ . ----------------

Now we pay attention to the follows of Theorem 1. and 2. for the twin prime problems.
From the Theorem 1. we have the following theorem:

Theorem 3.

$p \langle q$ are twin primes (greater than 3) iff $p = 6k - 1, q = 6k + 1$ and k convenient natural number.

Corollary 3.1.

(3.1.) If *p, q* are twin primes, then *pq = (6k-1)(6k+1)* = $36k^2 - 1$

Thus we give the followig theorem:

Theorem 4.

$(36k^2 - 1)$ hase exactly two prime factors iff *6k-1* and *6k+1* are twin primes.

Corollary 4.1.

There are finite number of twin primes iff there exist a K threshold number, then every k greater than K implies that $36k^2 - 1$ has greater or equal than three prime factors.

By this state follows that either *6k-1* or *6k+1* is composite number (or both), which allowable iff k has the form bellow:

(4.1) *k=6uv+u+v* or *k=6uv-u-v* or *k=6uv-u+v* or *k=6uv+u-v*

Thus we give the followig theorem:

Theorem 5.

There are finite number of twin primes iff there exist a K threshold number, then every k greater than K implies that k has the form one of the (4.1) . It means than there are infinitely many such k .

This Theorem 5. is equivalent to S.W.Golomb's following theorem, which appeared as problem E969 in the May, 1951, issue of the American Mathematical Monthly:
"There are infinitely many twin primes if and only if there are infinitely many positive integers and all four combinations of signs are allowed."

$$n \neq 6uv \pm u \pm v \quad \text{where} \quad n, u, v \text{ all} \geq 1$$

References

[1] S.W.Golomb: On factoring Jevons' number
CRYPTOLOGIA, (vol XX. no.3.) 1996.

[2] W.S. Jevons: The Principles of Science: A Treatise on Logic and Scientific Method
Macmillan & Co., London, 1873. Second edition 1877.

[3] S.W.Golomb: Problem E969
American Mathematical Monthly, vol.58. no.5. p.338, May, 1951.

[4] Tamás Dénes: Complementary prime sive
PUre Mathematics and Applications, Vol.12 (2002), No. 2, pp. 197-207