A Minimal Prime Generating Theorem that suggests the Prime Difference is

$$O(\pi(p(n)^{1/2}))$$

Bhupinder Singh Anand[1]

We define a minimal prime generating algorithm which suggests that the Prime Difference, $d_P(n)$, is $O(\pi(p(n)^{1/2}))$.

Introduction

Do we necessarily *discover* the primes, as in the sieve of Eratosthenes, or can we also *generate* them sequentially?

In other words, given the first k primes, can we generate the prime difference, $d_P(k)$, without *directly* testing any number larger than $p(k)$ for primality?

We give an affirmative answer, and define two prime number generating algorithms based on the following theorems.

We show that one of these is a minimal prime generating algorithm, and conjecture that it suggests the prime difference is $O(\pi(p(n)^{1/2}))$.

1.1: A Prime Number Generating Theorem

Theorem 1: For any given natural number k, and all $i \leq k$, let $p(i)$ denote the i'th prime, and define the sequence $\{a_P(i): i = 1 \text{ to } k\}$ such that $0 < a_P(i) < p(i)$, and:

[1] The author is an independent scholar. E-mail: re@alixcomsi.com; anandb@vsnl.com. Postal address: 32, Agarwal House, D Road, Churchgate, Mumbai - 400 020, INDIA. Tel: +91 (22) 2281 3353. Fax: +91 (22) 2209 5091.

Created: Saturday, 2nd June 2007, 3:31:06 AM IST, by re@alixcomsi.com. Updated: Tuesday, 12th June 2007, 12:11:55 PM IST, by re@alixcomsi.com.

$p(k) + a_P(i) \equiv 0 \pmod{p(i)}$

Let $d_P(k)$ be such that, for all $0 < l < d_P(k)$, there is some i such that:

$l \equiv a_P(i) \pmod{p(i)}$.

Then $d_P(k)$ is the Prime Difference, defined by:

$p(k+1) - p(k) = d_P(k)$.

Proof: For all $0 < l < d_P(k)$, there is some i such that:

$p(k) + l \equiv 0 \pmod{p(i)}$.

Since, by Bertrand's Postulate ([HW60], p343), $p(k+1) < 2p(k)$ for all natural numbers k, it follows that:

$d_P(k) < p(k)$

Hence, $p(k) + d_P(k) < p(k)^2$, and so it is the prime $p(k+1)$□

1.2: A Minimal Prime Number Generating Theorem

Since a natural number, n, is prime if, and only if, it is not divisible by any prime p such that $p^2 < n$, the above is also a proof of the following *minimal* prime generating theorem.

Theorem 2: For any given natural number k, and all $i \leq k$, let $p(i)$ denote the i'th prime, and define the sequence $\{a_P(i)\text{: } i = 1 \text{ to } m\}$ such that $0 < a_P(i) < p(i)$, $p(m)^2 < p(k) < p(m+1)^2$, and:

$p(k) + a_P(i) \equiv 0 \pmod{p(i)}$

Let $d_P(k)$ be such that, for all $l < d_P(k)$, there is some i such that:

$l \equiv a_P(i) \pmod{p(i)}$.

Then $d_P(k)$ is the Prime Difference, defined by:

$p(k+1) - p(k) = d_P(k)$.

2: Trim numbers

The significance of Theorem 1 is seen in the following algorithm.

We define Trim numbers recursively by $t(1) = 2$, and $t(n+1) = t(n) + d_T(n)$, where $p(i)$ is the i'th prime and:

(i) $d_T(1) = 1$; $a_T(2, 1) = 1$:

(ii) $d_T(n)$ is the smallest even integer that does not occur in the n'th sequence:

$\{ a_T(n, 1), \ldots, a_T(n, n\text{-}1)\}$;

(iii) $j_i \geq 0$ is selected so that, for all $0 < i \leq (n\text{-}1)$:

$0 \leq a_T(n+1, i) = \{(a_T(n, i) - d_T(n) + j_i * p(i)\} < p(i)$

It follows that the Trim number $t(n+1)$ is, thus, a prime unless all its prime divisors are less than $d_T(n)$.

2.1: The Trim Number Algorithm

The following illustrates how Trim numbers are generated sequentially.

n	$t(n)$																		
1	2	2	3	5	7	11	13	17	19	23		29	31	37	41	43	47	53	59
2	3	1	**2**	5															
3	5	1	1	**2**	7														
4	7	1	2	3	**4**	11													
5	11	1	1	4	3	**2**	13												
6	13	1	2	2	1	9	**4**	17											
7	17	1	1	3	4	5	9	**2**	19										
8	19	1	2	1	2	3	7	15	**4**	23									
9	23	1	1	2	5	10	3	11	15	4	27								
10	**27**	1	**0**	3	1	6	12	7	11	19	2	29	<== 3^3						
11	29	1	1	1	6	4	10	5	9	17		**2**	31						
12	31	1	2	4	4	2	8	3	7	15		27	**6**	37					
13	37	1	2	3	5	7	2	14	1	9		21	25	**4**	41				
14	41	1	1	4	1	3	11	10	16	5		17	21	33	**2**	43			
15	43	1	2	2	6	1	9	8	14	3		15	19	31	39	**4**	47		
16	47	1	1	3	2	8	5	4	10	22		11	15	27	35	39	**6**	53	
17	53	1	1	2	3	2	12	15	4	16		5	9	21	29	33	41	**6**	59

We consider any row, say, the k'th, which has no zeros.

		$p(1)$	$p(2)$	...	$p(n\text{-}1)$	$p(n)$
k	$p(n)$	$a(1, k)$	$a(2, k)$	...	$a(n\text{-}1, k)$	$r(n)$

Here, for $i < n$, $0 < a(i, k) < p(i)$:

(*i*) k is the number of the construction;

(*ii*) n is the number of the prime generated by the (k-1)th construction;

(*iii*) $a(i, k)$ is given by $p(n) + a(i, k) \equiv 0 \pmod{p(i)}$;

(*iv*) $r(n)$ is the least even integer not among the $a(i, k)$'s.

To obtain the (k+1)th row, subtract $r(n)$ from each $a(i, k)$ to give $a(i, k+1)$, adding $p(i)$ as many times as necessary to obtain a non-negative residue. Subtract $r(n)$ from $p(n)$ to give $a(n, k+1)$.

If $p(n) + r(n)$ is not congruent to 0, (mod $p(i)$), for any $i \leq n$, it is the prime $p(n+1)$.

Further, $p(n) + r(n)$ will not be prime only when $r(n)$, though not equal to any $a(i, k)$, nevertheless, exists in some residue class $\{a(i, k)\}$.

In this case, one of the $a(i, k+1)$ will be zero, and we have generated a composite number.[2]

2.3: A Trim Number Theorem

Theorem 3: For all $n > 1$, $t(n) < n^2$.

Proof: $t(n) - \{t(n\text{-}1) = d_T(n\text{-}1)\}$

$$d_T(n\text{-}1) < 2(n\text{-}1)$$

---

[2] We note that every time $r(n) = 2$, a prime pair occurs. Whilst if in any row $a(1) = 1$, and $a(i)$ is not 0 or 1 for any other i, then the construction has generated a prime of the form 2^m+1. Clearly, some problems regarding primes can be conveniently translated into problems about the residues $a(i)$ and the differences $r(n)$.

$t(n) - t(n-1) < 2(n-1)$

$t(n) - 2 < 2(n-1) + 2(n-2) + \ldots + 2(1)$

$t(n) < [2 + 2\{(n-1)*n/2\}]$

$t(n) < (n^2 - n + 2)$

Hence, for all $n > 1$, $t(n) < n^2$□

2.3: ... and two conjectures

Conjecture 1: For all k, $t(k) \leq p(n) \leq t(k+1)$ for some n.

Conjecture 2: If $p(n+1) = \{p(n) + d_P(n)\}$, then $d_P(n) = O(n)$.

2.4: Are the theorems significant?

The significance of the above theorems lies in the following observation [Ca05]:

> "Is there always a prime between n^2 and $(n+1)^2$? In 1882 Opperman stated $\pi(n^2+n) > \pi(n^2) > \pi(n^2-n)$, $(n>1)$, which also seems very likely, but remains unproven ([Ri95], p248).
>
> Both of these conjectures would follow if we could prove the conjecture that the prime gap following a prime p is bounded by a constant times $(\log p)^2$."

3: Compact numbers

The significance of Theorem 2 is seen in the following *minimal*[3] prime generating algorithm.

---

[3] The minimality is assured in the following argument by defining the indexing sequence $\{b_C(n, m), \ldots\}$, all of whose initial values are 0 for all natural numbers n and m. We then define $b_C(n, r) = r$ if $a_C(n, m) = r$. To find the least even integer that is absent in the sequence $\{a_C(n, 1), \ldots, a_C(n, k)\}$, we simply look for the smallest i such that $b_C(n, 2i) = 0$. It is easy to see that these conditions are, both, necessary and sufficient for generating the next Compact number.

The minimality aspect of the above argument was the focus of this paper as originally conceived. It is reflected in the abstract submitted to the International Congress of Mathematicians , August 3-11,1986, Berkeley, California, USA, and appears in the Book of Abstracts (p63) which was distributed at ICM-86.

"*A minimal prime generating algorithm*: Given (i) A set Q of k positive integers larger than 1 where Q(1) < Q(2) < … < Q(k), (ii) A set S of positive integers and (iii) A test T by which it can be determined for any

Compact numbers are defined recursively by $c(1) = 2$, and $c(n+1) = c(n) + d_C(n)$, where $p(i)$ is the i'th prime and:

(*i*) $d_C(1) = 1$, and $a_C(2, 1) = 1$;

(*ii*) $d_C(n)$ is the smallest even integer that does not occur in the n'th sequence:

$$\{a_C(n, 1), \ldots, a_C(n, k)\};$$

(*iii*) $j_i \geq 0$ is selected so that, for all $0 < i \leq k$:

$$0 \leq a_C(n+1, i) = \{ a_C(n, i) - d_C(n) + j_i * p(i)\} < p(i);$$

(*iv*) k is selected so that:

$$p(k)^2 < c(n) \leq p(k+1)^2;$$

(*v*) if $c(n) = p(k+1)^2$, then:

$$a_C(n, k+1) = 0.$$

It follows that the compact number $c(n+1)$ is either a prime, or a prime square, unless all, except a maximum of 1, prime divisors of the number are less than $d_C(n)$.

Q(i) whether it divides an integer x of S, we see that the number of tests needed to sieve out the multiples of Q(1), Q(2), …, Q(k) from S is a minimal iff the order of sieving is such that, if i is less than j, then the multiples of Q(i) are sieved out before those of Q(j).

We develop a modified Eratosthenes sieve in matrix form which is shown to be a minimal prime generating algorithm by the above lemma.

The 'Compact' algorithm is used to evaluate selected number theoretic functions."

However the paper, itself, could not be completed and submitted.

3.1: The Compact Number Algorithm

The following illustrates how Compact Numbers are generated sequentially.

n	*c*(*n*)	*a*(..)	*d*(*i*)	**3**	**5**	**7**	**11**	**13**	**17**	**<== Interval floor prime for p > 2**
1	2	**2**	**3**	**5**	**7**	**11**	**13**	**17**	**19**	**<== Interval ceiling prime for p > 2**
2	3	1	2	5						
3	5	1	2	7						
4	7	1	2	**9**	**25**					**<== End of first interval**
5	**9**	1	**0**	2	11					<== 3 x 3 : Prime square
6	11	1	1	2	13					
7	13	1	2	4	17					
8	17	1	1	2	19					
9	19	1	2	4	23					
10	23	1	1	2	**25**	**49**				**<== End of second interval**
11	**25**	1	2	**0**	4	29				<== 5 x 5 : Prime square
12	29	1	1	1	2	31				
13	31	1	2	4	6	37				
14	37	1	2	3	4	41				
15	41	1	1	4	2	43				
16	43	1	2	2	4	47				
17	47	1	1	3	2	**49**	**121**			**<== End of third interval**
18	**49**	1	2	1	**0**	4	53			<== 7 x 7 : Prime square
19	53	1	1	2	3	4	57			
20	**57**	1	**0**	3	6	2	59			<== 3 x 19 : Compact composite
21	59	1	1	1	4	2	61			
22	61	1	2	4	2	6	67			
23	67	1	2	3	3	4	71			
24	71	1	1	4	6	2	73			
25	73	1	2	2	4	6	79			
26	79	1	2	1	5	4	83			
27	83	1	1	2	1	4	87			
28	**87**	1	**0**	3	4	2	89			<== 3 x 29 : Compact composite
29	89	1	1	1	2	4	93			
30	**93**	1	**0**	2	5	4	97			<== 3 x 31 : Compact composite
31	97	1	2	3	1	4	101			
32	101	1	1	4	4	2	103			
33	103	1	2	2	2	4	107			
34	107	1	1	3	5	2	109			
35	109	1	2	1	3	4	113			
36	113	1	1	2	6	4	117			
37	**117**	1	**0**	3	2	4	**121**	**169**		<== 3 x 39 : Compact composite / **End of fourth interval**
38	**121**	1	2	4	5	**0**	6	127		<== 11 x 11 : Prime square
39	127	1	2	3	6	5	4	131		
40	131	1	1	4	2	1	6	137		
41	137	1	1	3	3	6	2	139		
42	139	1	2	1	1	4	6	145		

43	**145**	1	2	**0**	2	9	4	149		<== 5 x 29 : Compact composite
44	149	1	1	1	5	5	2	151		
45	151	1	2	4	3	3	6	157		
46	157	1	2	3	4	8	6	163		
47	163	1	2	2	5	2	4	167		
48	167	1	1	3	1	9	2	**169**	**289**	**<== End of fifth interval**
49	**169**	1	2	1	6	7	**0**	4	173	<== 13 x 13 : Prime square
50	173	1	1	2	2	3	9	4	177	
51	**177**	1	**0**	3	5	10	5	2	179	<== 3 x 59 : Compact composite
52	179	1	1	1	3	8	3	2	181	
53	181	1	2	4	1	6	1	8	189	
54	**189**	1	**0**	1	**0**	9	6	2	191	<== 3 x 3 x 3 x 7 : Compact\Trim composite
55	191	1	1	4	5	7	4	2	193	
56	193	1	2	2	3	5	2	4	197	
57	197	1	1	3	6	1	11	2	199	
58	199	1	2	1	4	10	9	6	205	
59	**205**	1	2	**0**	5	4	3	6	211	<== 5 x 41 : Compact composite
60	211	1	2	4	6	9	10	8	219	
61	**219**	1	**0**	1	5	1	2	4	223	<== 3 x 73 : Compact composite
62	223	1	2	2	1	8	11	4	227	
63	227	1	1	3	4	4	7	2	229	
64	229	1	2	1	2	2	5	4	233	
65	233	1	1	2	5	9	14	4	237	
66	**237**	1	**0**	3	1	5	10	2	239	<== 3 x 79 : Compact composite
67	239	1	1	1	6	3	8	2	241	
68	241	1	2	4	4	1	6	8	249	
69	**249**	1	**0**	1	3	4	11	2	251	<== 3 x 83 : Compact composite
70	251	1	1	4	1	2	9	6	257	
71	257	1	1	3	2	7	3	4	261	
72	**261**	1	**0**	4	5	3	12	2	263	<== 3 x 87 : Compact composite
73	263	1	1	2	3	1	10	4	267	
74	**267**	1	**0**	3	6	8	6	2	269	<== 3 x 89 : Compact composite
75	269	1	1	1	4	6	4	2	271	
76	271	1	2	4	2	4	2	6	277	
77	277	1	2	3	3	9	9	4	281	
78	281	1	1	4	6	5	5	2	283	
79	283	1	2	2	4	3	3	6	**289**	**<== End of sixth interval**

(*Total numbers generated: 79; Primes: 61; Prime squares: 5; Composites: 13*)

3.2: Two compact number theorems

Theorem 4: There is always a compact number $c(m)$ such that:

$$n^2 < c(m) \leq (n+1)^2.$$

Proof: If $p(k) \leq n < p(k+1)$, then $(n+1) \leq p(k+1)$.

Now $\{(n+1)^2 - n^2\} = \{2n + 1\} > 2p(k) > 2k$.

Hence $(n+1)^2 > \{n^2 + 2k\}$.

Since there is always a compact number in any interval larger than $2k$ between $p(k)^2$ and $p(k+1)^2$, the theorem follows□

Theorem 5: For sufficiently large n, $d_C(n) <$ constant$*\{c(n)/\log c(n)\}^{1/2}$

Proof: By definition, $d_C(n) \leq 2k$, where $p(k)^2 < c(n) \leq p(k+1)^2$.

The theorem follows from the Prime Number Theorem, since k is the number of primes less than $c(n)^{1/2}$□

3.3: ... and two more conjectures

Conjecture 3: If $p(k)^2 < p(n) < p(k+1)^2$, then:

$$\begin{aligned} \{p(n+1) - p(n)\} &= \mathrm{O}(\mathrm{k}) \\ &= \mathrm{O}(\pi(p(n)^{1/2})). \end{aligned}$$

Conjecture 4: $\lim^{\sup}_{n\to\infty}$ {Number of primes $< n$}/{Number of compacts $< n$} = 1/2.

References

[An64] Anand, B. S. 1964. *Two Series containing the Primes and a Conjecture concerning the Prime Difference*. Transcribed notes.

<http://alixcomsi.com/Prime_number_generator.htm>

[Ca05] Caldwell, Chris. K. 2005. *Prime Conjectures and Open Questions*. Web resource.

<http://www.utm.edu/research/primes/notes/conjectures/>

[HW60] Hardy, G. H. and Wright, E. M. 1960. *An Introduction to the Theory of Numbers*. 4th edition. Clarendon Press, Oxford.

[Ri95] Ribenboim, P. 1995. *The new book of prime number records.* 3rd edition, Springer-Verlag, New York, NY, pp. xxiv+541, ISBN 0-387-94457-5. 1995.