Notes on Number Theory and Discrete Mathematics
ISSN 1310-5132
Vol. 21, 2015, No. 4, 22–29

Two triangular number primality tests and twin prime counting in arithmetic progressions of modulus 8

Werner Hürlimann

Swiss Mathematical Society, University of Fribourg
1700 Fribourg, Switzerland
e-mail: whurlimann@bluewin.ch

Abstract: Two triangular number based primality tests for numbers in the arithmetic progressions $8n \pm 1$ are obtained. Their use yield a new Diophantine approach to the existence of an infinite number of twin primes of the form $(8n-1, 8n+1)$.

Keywords: Primality test, Compositeness test, Triangular number, Arithmetic progression, Diophantine curve of degree two, Divisor function, Twin prime.
AMS Classification: 11A51, 11B25, 11D85.

1 Introduction

According to [1], Chapter 4, one distinguishes between *primality tests* and *compositeness tests*. Given a number *N*, a successful primality test on it proves that *N* is prime, and a successful compositeness test proves that *N* is composite. A stringent primality test states a condition on *N*, which implies that *N* is prime if it is fulfilled and *N* is composite otherwise. Usually, primality tests are often quite complicated (e.g. the Rabin-Miller test or the AKS test by [2], as presented in [3]) or only applicable to numbers of a special form. For a brief history before the computer age consult [4].

The considered triangular number based primality tests apply only to numbers that belong to the two arithmetic progressions $8n \pm 1$. They exploit a relationship between numbers from these sequences and *triangular numbers* of the form $\frac{1}{2}m(m+1)$ (sequence A000217 in the OEIS [5]). In Section 2, we consider the infinite matrix $S = (S_{k,j})$ of *triangular S-numbers* defined by $S_{k,j} = f(k, j)$, $k = 1,2,...,\ j = 1,2,...$, where

$$f(x, y) = (x-1)(2y+1) + \tfrac{1}{2}y(y+1), \quad x, y = 1,2,...,$$

is a binary function of degree two. We prove that $8n+1$ is prime if, and only if, the number n is not an S-number. Moreover, composite numbers $8n+1$ are always generated by S-numbers n. Section 3 considers a similar infinite partially truncated matrix $T = (T_{k,j})$ of *triangular T-numbers* and derives a primality test for numbers in the arithmetic progression $8n-1$. Applications to twin primes follow in Section 4.

2 Primality test for numbers in the arithmetic progression 8*n* + 1

Starting point is the binary function of degree two defined by

$$f(x, y) = (x-1)(2y+1) + \tfrac{1}{2}y(y+1), \quad x, y = 1,2,..., \tag{2.1}$$

which is an affine transform of triangular numbers $\frac{1}{2}y(y+1)$ and odd numbers $2y+1$. Consider the infinite matrix of natural numbers $S = (S_{k,j}), k = 1,2,..., j = 1,2,...$, called *triangular S-numbers*, which are defined by

$$S_{k,j} = f(k, j), \quad k = 1,2,..., i = 1,2,... \ . \tag{2.2}$$

We claim that S-numbers of the form $S_{k,j} = n$ for some (k, j) always generate composite numbers in the arithmetic progression $8n+1$, and that natural numbers n, which cannot be represented as $S_{k,j} = n$, necessarily lead to prime numbers of the form $8n+1$. The first assertion is almost trivial in view of the identity

$$8f(x, y) + 1 = \big(2y+1\big) \cdot \big(2y+1+8(x-1)\big), \quad x, y = 1,2,.... \tag{2.3}$$

The second assertion is less elementary but not very difficult to show. What is remarkable is the fact that the stated conditions characterize the totality of prime and composite numbers in this special arithmetic progression.

Theorem 2.1 (Primality test with triangular S-numbers). *A natural number in the arithmetic progression* $8n+1, n = 1, 2,...,$ *is prime if, and only if,* n *is not a triangular S-number.*

Proof. By definition (2.2), it suffices to show that the Diophantine curve of degree two $f(x, y) = n$ has positive integral solutions $x, y \geq 1$ if, and only if, the number $N = 8n+1$ is composite. To solve this Diophantine curve of degree two we closely follow the method in [6], Section 6.1. The equation $f(x, y) = n$ is of the form

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{2.4}$$

with coefficients $a = 0, b = 2, c = \frac{1}{2}, d = 1, e = -\frac{3}{2}, f = -(1+n)$. Since $4ac - b^2 = -4$ is negative, the curve (2.4) is a hyperbola. Multiply (2.4) with $4c(4ac - b^2) = -8$ and consider the transformation of variables

$$x' = (4ac - b^2)x + 2cd - be = -4(x-1), \quad y' = bx + 2cy + e = 2x + y - \tfrac{3}{2},$$

which implies that (2.4) is equivalent with the equation $4y'^2 - x'^2 = N, N = 8n+1$. Setting further $x' = \pm X$, $y' = \pm\frac{1}{2}Y$, one obtains the equation $Y^2 - X^2 = N$. Let now $N = 8n+1 = p$ be a prime, and set $Y - X = t, Y + X = d$. The equation $t \cdot d = p$ has the solutions $(t,d) = (1,p)$ or $(t,d) = (p,1)$, hence $x' = \pm X = \pm\frac{p-1}{2} = \pm 4n$, $y' = \pm\frac{1}{2}Y = \pm\frac{p+1}{4} = \pm(2n+\frac{1}{2})$. To make $x > 0$, $y \geq 0$ choose $x' = -4n$, $y' = 2n+\frac{1}{2}$. Then, transforming back, one obtains $x = n+1$, $y = 0$, which shows that *n* is not of the form $S_{k,j}$ in (2.2). Therefore, if $N = 8n+1 = p$ is a prime, then *n* is not an *S*-number. It remains to show that if $N = 8n+1$ is composite, then n is an *S*-number. Since N is odd this number contains a factor of the form $t = 2i+1 \leq \sqrt{N}$ for some $i = 1, 2, \ldots$. The cofactor d such that $t \cdot d = N$ satisfies the inequalities $d \geq \sqrt{N} \geq t$, hence $d = 2i+1+z$ for some natural number $z \geq 0$. It follows that

$$N = t \cdot d = (2i+1)\cdot(2i+1+z) = (2i+1)^2 + (2i+1)\cdot z = 8\cdot\tfrac{1}{2}i\cdot(i+1) + 1 + (2i+1)\cdot z .$$

To be of the form $N = 8n+1$ one must have $z = 8(k-1)$ for some $k = 1,2,\ldots$. It follows that $N = 8n+1 = (2i+1)\cdot(2i+1+8(k-1))$ and n is an S-number by the identity (2.3). □

Remark 2.1. As an immediate application, it follows from Theorem 2.1 and the identity (2.3) that $N = 8n+1$ is a square if, and only if, one has $x = 1$ in (2.3), that is $n = \frac{1}{2}y(y+1)$ belongs to the sequence of triangular numbers, and necessarily $N = (2i+1)^2$.

3 Primality test for numbers in the arithmetic progression 8*n* – 1

Given is the binary function of degree two

$$g(x,y) = (x-1)(2y+1) - \tfrac{1}{2}y(y+1), \quad x, y = 1,2,\ldots, \tag{3.1}$$

which is also an affine transform of triangular numbers $\frac{1}{2}y(y+1)$ and odd numbers $2y+1$. Consider the infinite truncated matrix of natural numbers $T = (T_{k,j})$, $k = 2, 3, \ldots$, $j = 1, 2, \ldots, 2k-3$ called *triangular T-numbers*, which are defined by

$$T_{k,j} = g(k,j), \quad k = 2,3,\ldots,\ j = 1,2,\ldots,2k-3 . \tag{3.2}$$

The truncation is motivated as follows. As in Section 1, we would like that *T*-numbers of the form $\underline{T}_{k,j} = n$ for some (k, j) always generate composite numbers in the arithmetic progression $8n-1$, and that natural numbers *n*, which cannot be represented as $\underline{T}_{k,j} = n$, necessarily lead to prime numbers of the form $8n-1$. Similarly to (2.3) one has the identity

$$8g(x,y) - 1 = (2y+1)\cdot(8(x-1) - (2y+1)), \quad x, y = 1,2,\ldots . \tag{3.3}$$

If $2y+1$ is prime this expression will generate composite numbers only if the second factor exceeds one, that is $y \leq 4x-6$. Now, for $y \leq 2x-3$, one sees easily that $g(x,y)$ is

strictly positive and strictly increasing such that $g(x,y) > g(x,y-1)$. For $2x-3 < y \le 4x-6$ the sequence is strictly decreasing and satisfies the symmetry relation

$$g(x, 2x-3+y) = g(x, 2x-2-y), \quad y = 1, 2, ..., 2x-3. \tag{3.4}$$

Therefore, it suffices to define triangular *T*-numbers for $k = 2, 3, ...,\ j = 1, 2, ..., 2k-3$. Again, triangular *T*-numbers completely characterize the totality of prime and composite numbers in the arithmetic progression $8n-1$.

Theorem 3.1 (Primality test with triangular T-numbers). *A natural number in the arithmetic progression* $8n-1, n = 1, 2, ...,$ *is prime if, and only if,* n *is not a triangular T-number.*

Proof. We show that the Diophantine curve of degree two $g(x,y) = n$ has integral solutions $x = 2, 3, ...,\ y = 1, 2, ..., 2x-3$ if, and only if, the number $N = 8n-1$ is composite. With $a = 0, b = 2, c = -\frac{1}{2}, d = 1, e = -\frac{5}{2}, f = -(1+n)$, the equation $g(x,y) = n$ is of the form

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{3.5}$$

Since $4ac - b^2 = -4$ is negative, the curve (3.5) is a hyperbola. Multiply (3.5) with $4c(4ac-b^2) = 8$ and consider the transformation of variables

$$x' = (4ac-b^2)x + 2cd - be = -4(x-1), \quad y' = bx + 2cy + e = 2x - y - \tfrac{5}{2},$$

which implies that (3.5) is equivalent with the equation $x'^2 - 4y'^2 = N,\ N = 8n-1$. Setting $x' = \pm X,\ y' = \pm\frac{1}{2}Y$, one obtains the equation $X^2 - Y^2 = N$. Now, let $N = 8n-1 = p$ be a prime, and set $X - Y = t,\ X + Y = d$. Solving the equation $t \cdot d = p$, one gets $(t,d) = (1,p)$ or $(t,d) = (p,1)$. It follows that $x' = \pm X = \pm\frac{p+1}{2} = \pm 4n,\ y' = \pm\frac{1}{2}Y = \pm\frac{p-1}{4} = \pm(2n-\frac{1}{2})$. To make $x > 0,\ y \ge 0$ choose $x' = -4n,\ y' = 2n - \frac{1}{2}$. Transforming back, one has $x = n+1,\ y = 0$, hence n is not of the form $T_{k,j}$ in (3.2). Therefore, if $N = 8n-1 = p$ is a prime, then *n* is not a *T*-number. It remains to show that if $N = 8n-1$ is composite, then *n* is a *T*-number. Since N is odd, it contains a prime factor $t = 2i+1$ for some $i = 1,2,...$. The cofactor d such that $t \cdot d = N$ can be written as $d = z - (2i+1)$ for some natural number $z > (2i+1)$. It follows that

$$N = t \cdot d = (2i+1)\cdot(z-(2i+1)) = (2i+1)\cdot z - (2i+1)^2 = (2i+1)\cdot z - 8\cdot\tfrac{1}{2}i\cdot(i+1) - 1.$$

To be of the form $N = 8n-1$ one must have $z = 8(k-1)$ for some $k = 2,3,...$. It follows that $N = 8n-1 = (2i+1)\cdot(8(k-1)-(2i+1))$. The second factor is non-trivial if $i \le 4k-6$, and by the symmetry relation (3.4) an index $i \le 2k-3$ will do. This shows *n* is a *T*-number. □

4 Counting *S*- and *T*-numbers: Application to twin primes

We state some counting formulas for *S*- and *T*-numbers and apply them to determine the number of twin primes $(8n-1, 8n+1)$ in finite sets $\{1, 2, ..., N\}$. The following notations are used:

$S_c(N)$: The set of S-numbers in $\{1, 2, ..., N\}$ such that $8n+1$ is composite

$T_c(N)$: The set of T-numbers in $\{1, 2, ..., N\}$ such that $8n-1$ is composite

$S_p(N) = \overline{S_c(N)}$: The set of $n \in \{1,2,...,N\}$ such that $8n+1$ is prime (complement of $S_c(N)$ in $\{1, 2, ..., N\}$)

$T_p(N) = \overline{T_c(N)}$: The set of $n \in \{1,2,...,N\}$ such that $8n-1$ is prime (complement of $T_c(N)$ in $\{1, 2, ..., N\}$)

The intersection $S_p(N) \cap T_p(N)$ consists of those $n \in \{1,2,...,N\}$ such that $(8n - 1, 8n + 1)$ is a twin prime. With $|M|$ the cardinality of the set M, one obtains the counting formula

$$\begin{aligned} |S_p(N) \cap T_p(N)| &= \left|\overline{S_c(N)} \cap \overline{T_c(N)}\right| = \left|\overline{S_c(N)}\right| + \left|\overline{T_c(N)}\right| - \left|\overline{S_c(N)} \cup \overline{T_c(N)}\right| \\ &= |S_p(N)| + |T_p(N)| - \left|\overline{S_c(N) \cap T_c(N)}\right| = |S_p(N)| + |T_p(N)| + |S_c(N) \cap T_c(N)| - N. \end{aligned} \tag{4.1}$$

Theorem 4.1 (Twin prime conjecture in arithmetic progressions of modulus 8) *There exists an infinity of twin primes* $(8n-1,8n+1)$ *if, and only if, the following inequality holds*:

$$|S_p(N)| + |T_p(N)| + |S_c(N) \cap T_c(N)| > N \text{, for all } N \geq 3. \tag{4.2}$$

In fact (4.1) holds for arbitrary arithmetic progressions $qn \pm 1$ if one identifies the sets $S_c(N)$, $T_c(N)$ as composite numbers, and $S_p(N)$, $T_p(N)$ as primes in $qn \pm 1$. What is special here is the Diophantine interpretation. The set $S_c(N) \cap T_c(N)$ represents the $n \in \{1,2,...,N\}$ that are simultaneously *S*- and *T*-numbers. From the given proofs one sees that $S_c(N) \cap T_c(N)$ coincides with the numbers $n \in \{1,2,...,N\}$ such that the intersection of the two hyperbolas

$$Y^2 - X^2 = 8n+1, \quad U^2 - V^2 = 8n-1, \tag{4.3}$$

have integral solutions (X, Y, U, V) that satisfy the conditions

$$\begin{aligned} &x = 1 + \tfrac{X}{12} \in \{1,2,...\}, \quad y = \tfrac{1}{6}(Y \pm 1 - X) \in \{1,2,...\}, \\ &u = 1 + \tfrac{U}{12} \in \{1,2,...\}, \quad v = \tfrac{1}{6}(U \pm 1 - V) \in \{1,2,...,2u-3)\}. \end{aligned} \tag{4.4}$$

Alternatively, and this holds for arbitrary arithmetic progressions $qn \pm 1$, the cardinality of the set $S_c(N) \cap T_c(N)$ is determined by the following formula (as usual $d(n)$ denotes the divisor function, and $1\{\cdot\}$ is the indicator function)

$$\left|S_c(N) \cap T_c(N)\right| = \sum_{n=1}^{N} 1\{d(qn-1)>2\} \cdot 1\{d(qn+1)>2\}. \qquad (4.5)$$

Table 1 illustrates Theorem 4.1 for a small sample of computed values (to evaluate (4.5) use the sequence A000005 in Sloane's OEIS).

N	$\left\|S_p(N)\right\|$	$\left\|T_p(N)\right\|$	$\left\|S_c(N) \cap T_c(N)\right\|$	$\left\|S_p(N) \cap T_p(N)\right\|$
300	81	90	143	14
1500	341	366	845	52
3000	656	668	1760	84
6000	1209	1241	3704	154
9000	1763	1792	5666	221
12000	2294	2320	7671	285

Table 1. Number of twin primes in selected intervals

Together with the characterizations Theorems 3.1 and 4.1 the definition of the *S*- and *T*-numbers in (2.2) and (3.2) can be used for the algorithmic generation of twin primes $(8n-1,8n+1)$ below a limit $n \le N$. Applying a sieve, it suffices to eliminate all *S*- and *T*-numbers below $n \le N$. The remaining $n \in \{1,2,...,N\}$ yield the primes of the form $8n+1$ respectively $8n-1$, and those common values of $n \in \{1,2,...,N\}$ yield the twin primes. Table 2 illustrates.

71	2087	4127	6959	10271	15647	20231
191	2111	4271	7127	11159	15887	20639
239	2591	4799	7487	11351	16631	20807
311	2687	4967	7559	11831	17207	21191
431	2711	5231	8087	12071	18047	21599
599	2999	5279	8231	12239	18119	21647
1031	3119	5519	8999	13007	18287	21839
1151	3167	5639	9239	13679	18311	22271
1319	3359	5879	9431	14447	18911	22367
1487	3527	6359	9719	14591	19079	23039
1607	3671	6551	9767	15287	19751	23687
1871	3767	6791	10007	15359	19991	23831

Table 2. Twin primes $(8n-1,8n+1)$ below $n \le N = 3000$ (first primes are listed)

Remark 4.1. Twin primes $(8n-1, 8n+1)$ are special in the sense that they are always of the form $(24k-1, 24k+1)$. Indeed, if $n = 3k+1$ then $8n+1 = 24k+9$ is divisible by 3, and if $n = 3k+2$ then $8n-1 = 24k+15$ is also divisible by 3.

Finally, the defined triangular *S*- and *T*-numbers suggest two new strategies to prove the twin prime conjecture. By Dirichlet's theorem on the number of primes in arithmetic progressions, the asymptotic behaviour for the first two terms in (4.1) is known (e.g. [1], formula (2.40)). Therefore, one must further determine the asymptotic behaviour of the numbers $n \in \{1,2,...,N\}$ satisfying the Diophantine conditions (4.3) – (4.4) when $N \to \infty$ or obtain a sufficiently high lower bound for it. Equivalently, one must find an asymptotic formula or a lower bound that count the number of distinct *S*- and *T*-numbers. To achieve this seems difficult, and goes beyond the present investigation. However, readers specialized in the derivation of asymptotic formulas might appreciate these new possibilities.

Remark 4.2. For different purposes, it might be interesting to consider the sets that count the number of different representations or solutions to the Diophantine equations $f(x,y) = n$ and $g(x,y) = n$. These sets can be viewed as generalized sets of *S*- and *T*-numbers that are denoted by $S_c^{mult}(N)$ respectively $T_c^{mult}(N)$. They count each *S*- or *T*-number according to its multiplicity taking into account the number of different solutions to the stated equations. It is not difficult to derive the following counting formulas for them (as usual $\lfloor \cdot \rfloor$ denotes the floor function)

$$\left|S_c^{mult}(N)\right| = \sum_{n=1}^{N}\left(\left\lfloor \frac{d(8n+1)+1}{2} \right\rfloor - 1\right)_+ , \quad \left|T_c^{mult}(N)\right| = \sum_{n=1}^{N}\left(\left\lfloor \frac{d(8n-1)+1}{2} \right\rfloor - 1\right)_+ . \tag{4.6}$$

Table 3 illustrates computation.

N	$\left\|S_c(N)\right\|$	$\left\|S_c^{mult}(N)\right\|$	$\left\|T_c(N)\right\|$	$\left\|T_c^{mult}(N)\right\|$
300	219	412	210	398
1500	1159	2630	1134	2601
3000	2344	5758	2332	5723
6000	4791	12538	4759	12477
9000	7237	19691	7208	19634
12000	9706	27117	9680	27033

Table 3. Counting *S*- and *T*-numbers without and with multiplicity in selected intervals

To conclude, we like to point out that different elementary twin prime characterization theorems have been obtained in [7] and [8].

References

[1] Riesel, H. (1985) *Prime Numbers and Computer Methods for Factorization* (2nd ed. 1994), Birkhäuser, Basel.

[2] Agrawal, M., Kayal, N. & Saxena, N. (2004) PRIMES is in P, *Annals Math*., 160(2), 781–793.

[3] Schoof, R. (2008) Four primality testing algorithms, In: Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, *Math. Sci. Res. Inst. Publ., Survey in Number Theory*, Vol. 44, 101–126, Cambridge University Press, Cambridge.

[4] Mollin, R. A. (2002) A brief history of factoring and primality testing B.C. (before computers), *Mathematics Magazine*, 75(1), 18–29.

[5] Sloane, N. J. A. (1964) *The On-Line Encyclopedia of Integer Sequences*, `https://oeis.org/`

[6] Krätzel, E. (1981) *Zahlentheorie*, Mathematik für Lehrer, Band 19, VEB Deutscher Verlag für Wissenschaften, Berlin.

[7] Dilcher, K. & Stolarsky, K.B. (2005) A Pascal-type triangle characterizing twin primes, *Amer. Math. Monthly*, 112, 673–681.

[8] Königsberg, S. R. (2011) Characterizations of prime k-tuples using binomial expressions, *Int. Math. Forum*, 6(44), 2165–2168.