NNTDM 10 (2004), 4 100-105

AN EXTENSION OF EULER'S PRIME-GENERATING FUNCTION

J. V. Leyendekkers
The University of Sydney, 2006, Australia

A. G. Shannon
Warrane College, The University of New South Wales, Kensington, 1465, &
KvB Institute of Technology, North Sydney, NSW 2060, Australia

Abstract

Using integer structure, six simple functions are obtained to give values for x that result in composite N in Euler's prime generating function

$$N = x^2 + x + p\,;$$

the remaining values for x yield primes. In $0 \le x \le 500$, with p=41, there are 314 values for x which generate primes, the formation of which follows an orderly pattern based on integer structure. All primes can be generated from N=6r±1, with specific values of r being rejected, in an analogous manner to the x values.

1. Introduction

About the year 1772, Euler [3] found that that the function

$$N = x^2 + x + p \tag{1.1}$$

where p=2,3,5,11,17,41, gave N as prime for $0 \le x \le p - 2$.

However, this function continues to generate primes for selected values of x, up to 'large' numbers. The values of x which yield composite values for N may be calculated using modular rings on the basis of integer structure as we shall show.

2. Composite N

Let

$$y = qp - x\,, \text{ with } q=1,2,3,4,\ldots\,. \tag{2.1}$$

Substitution of Equation (2.1) into Euler's Equation (1.1) gives

$$N = q^2 p^2 + p(q + 1 - 2qy) + y^2 - y. \tag{2.2}$$

Now let

$$N = (qp + a)(qp + b). \tag{2.3}$$

Equating (2.2) and (2.3) gives

$$a = \tfrac{1}{2q}\big(q(1-2y)+1\big) + \tfrac{1}{2q}\big(q(q+2-4y)+1\big)^{1/2}, \tag{2.4}$$

and

$$b = \tfrac{1}{2q}\left(q(1-2y)+1\right) - \tfrac{1}{2q}\left(q(q+2-4y)+1\right)^{1/2}. \tag{2.5}$$

Case 1: q=1.
In this case,

$$\begin{aligned} a &= (1-y) + (1-y)^{1/2}, \\ b &= (1-y) - (1-y)^{1/2}. \end{aligned} \tag{2.6}$$

We need to consider when (1-y) is a square, because integer values for a and b yield composite values for N. An analysis of squares is most easily done by using the modular ring Z_4 since squares are only found in the classes $\bar{0}_4$ (even) and $\bar{1}_4$ (odd) [5].

(1-y) odd. When (1-y) is odd but not divisible by 3, the squares in Z_4 are given by [7,8]:

$$(1-y) = 4R_1 + 1. \tag{2.7}$$

with

$$R_1 = 6K_j,\ j = 0,1,2,3,\ldots.$$

For j even,

$$K_j = \frac{1}{2}n(3n-1), \qquad \text{Class A;} \tag{2.8a}$$

for j odd,

$$K_j = \frac{1}{2}n(3n+1), \qquad \text{Class B;} \tag{2.8b}$$

but

$$R_1 = (1+3n)(2+3n),\ n = 0,1,2,3,\ldots, \quad \text{Class C} \tag{2.8c}$$

if 3|(1-y).
On substituting Equation (2.7) into Equation (2.1) we get the x values which yield composites; that is,

$$x = p + 4R_1$$

as in Table 1.

(1-y) even. All even squares in Z_4 are given by

$$N = 4R_0. \tag{2.9}$$

However, $(1-y)^{1/2} \in \{\bar{0}_4, \bar{2}_4\}$; that is,

$$\left.\begin{aligned} (1-y)^{1/2} &= 4r_0 \quad Class\ D \\ (1-y)^{1/2} &= 4r_2 + 2 \quad Class\ E \end{aligned}\right\} \tag{2.10}$$

so that

$$R_0 = \begin{cases} 4r_0^2, \ or \\ (2r_2+1)^2 \end{cases} with\ r_0, r_2 = 0,1,2,3,\ldots.$$

The various functions are summarised in Table 2.

(1-y)=kp. This is a special case with k=0,1,2,3,… .This case yields

$$a = kp + (kp)^{1/2},$$
$$b = kp - (kp)^{1/2},$$

so that

$$(p+a)(p+b) = p\{((k+1)^2 \times p) - k\}.$$

Thus N will be composite when

$$x = (1+k)p - 1$$

as in Table 3.

	A	B	C
R_1	$3n(3n\text{-}1)$	$3n(3n+1)$	$(1+3n)(2+3n)$
y	$-12n(3n\text{-}1)$	$-12n(3n+1)$	$-4(1+3n)(2+3n)$
x	$12n(3n\text{-}1)+p$	$12n(3n+1)+p$	$4(1+3n)(2+3n)+p$

Table 1: Values of x which yield composite N when (1-y) or square root function Equation (2.4) is odd

	D	E
R_0	$4r_0^2$	$(2r_2+1)^2$
y	$(1-16r_0^2)$	$(1-4(2r_2+1)^2)$
x	$(16r_0^2+(p-1))$	$16r_2(r_2+1)+(p+3)$

Table 2: Values of x which yield composite N when (1-y) or a square root function Equation (2.4) is even

(1-y)	Function for x	x	N (composite
EVEN D	$40+16r_0^2$	40,56,104,184,296,440, 616	1681,3233,10961,34081, 87953
E	$44+16r_2(r_2+1)$	44,76,140,236,364,524	2021,5893,19781,55973, 132901
ODD A	41+12n(3n-1)	41,65,161,329,569	1763,4331,26123,108611, 324371
B	41+12n(3n+1)	<u>41</u>,89,209,401,665	<u>1763</u>,8051,43931,161243, 442931
C	41+4(1+3n)(2+3 n)	49,121,265,481,769	2451,14803,70531,231883, 592171
= kp	41(1+k)-1	<u>40</u>,81,122,163,204,245, 286,327,368,409,450, 491,532	<u>1681</u>,6683,15047,26773, 41861,60311,82123, 107297,135833,167731, 202991,241613,283597

Table 3: Invalid values of x when p=41, q=1 (underlined values are duplicates)

<u>Case 2: q>1</u>

The same method as above can be used in this case. We distinguish the cases where q is even and odd.
When q is even, the square root function is always odd, so that

$$q(q+2-4y)+1 = 4R_1 + 1 \tag{2.12}$$

from which the value of y and hence of x can be found. The values for R_1 are taken from Table 1.

When q is odd, the square root function is even, except when an even square can be factored out to leave an odd residue. In this case Tables 1 and 2 might both be used. Thus

$$q(q+2-4y)+1 = 4R_0 \tag{2.13}$$

and in some cases Equation (2.12) is also needed (Table 4). Results for $0 \le x \le 500$ can be found in Table 4.

q	Functions for x*	Invalid x
2	$81+\frac{1}{2}R_1$	82,84,87,91,96,102,109,117,126,136,147,159,172,186,201,217,234,252, 271,291,312,334,357,381,406,432,459,487
3**	$\frac{1}{3}(365+R_0)$	122,123,127,130,138,143,155,162,178,187,207,218,242,255,283,298, 330,347,383,402,442,463
4	$164+\frac{1}{4}(R_1-6)$	163,164,170,173,185,190,208,215,239,248,278,289,325,338,380,395, 443,460
5	$205+\frac{4}{5}(R_1-2)$ $205+\frac{1}{5}(4R_0-9)$	205,213,237,261,309,349,421,477 216,232,268,300,360,408,492
6	$244+\frac{1}{6}R_1$	244,245,246,249,251,256,259,266,270,279,284,295,301,314,321,336, 344,361,370,389,399,420,431,454,466,491
7	$287+\frac{1}{7}(4R_1-15)$ $287+\frac{1}{7}(R_0-16)$	286,302,326,374,422 286,287,299,302,326,331,367,374,422,431,491
8	$328+\frac{1}{8}(R_1-20)$	327,328,342,345,373,378, ,427,483,492
9	$369+\frac{1}{9}(4R_1-24)$ $369+\frac{1}{9}(4R_0-25)$	369,385,425,473 368,388,420,480
10	$410+\frac{1}{10}(R_1-30)$	407,409,410,416,418,428,431,445,449,467,472,494,500
11	$451+\frac{1}{11}(4R_1-35)$ $451+\frac{1}{11}(4R_0-36)$	450,474 451,471
12	$492+\frac{1}{12}(R_1-42)$	489,491,492,496

Table 4: Underlined values are duplicates; * from Equations (2.12) and (2.13) and Tables 1 and 2; ** R_1 values are the same as those given by R_0 (E)

3. Final Remarks

Table 5 shows how the production of primes changes as x increases. Initially the production drops sharply, but then it stabilises around 50%. This suggests that primes will be produced up to large values of x. Table 6 shows changes of composite numbers with q.

Range of primes	Range of x	No. of primes generated
41-10141	0-100	86
10141-40241	101-200	70
40241-88547	201-300	53
92153-158843	301-400	60
162853-249541	401-500	55
251543-359441	501-600	56
361843-490741	601-700	49
497771-631271	701-800	51

Table 5: Production of primes

q	1	2	3	4	5	6	7	8	9	10	11	12
No. of composites	23	28	22	18	15	26	10	8	7	12	4	2

Table 6: Production of composites

Euler's results in isolation do not show the true picture. The distribution of primes is comparatively orderly when viewed from the perspective of the integer structure in the framework of modular rings. Essentially, Euler's function arises from the integer structure in an analogous manner to the simpler functions $6R\pm1$.

All the primes can be generated from $6R\pm1$, using values of R which are compatible with the integer structure. For example, just as certain values of x were shown to be invalid for primes, there are invalid values of R which are given by (Table 7) [6]

$$R = R' + pt,\ t = 0,1,2,3,.... \tag{3.1}$$

Class of N	Class of p	R'
$\overline{4}_6$	$\overline{2}_6$	$\frac{1}{6}(p-1)$
$N = 6R+1$	$\overline{4}_6$	
$\overline{2}_6$	$\overline{2}_6$	$\frac{1}{3}\left\{\frac{1}{2}(p+1)+p\right\}$
$N = 6R-1$	$\overline{4}_6$	$\frac{1}{3}\left\{\frac{1}{2}(p+1)+2p\right\}$

Table 7: Values for R'

When the class structure is taken into account, as has been done here, the building up of the primes is seen to be very straightforward. The reader might like to try p=17 in Equa-

tion (1.1). Finally, we note that the form of (1.1) is used by modern writers too [2], but [9] uses the form

$$x^2 - x + p. \tag{3.2}$$

In this case we use $y=x+1$, since

$$(x+1)^2 - (x+1) + p = x^2 + x + p.$$

For instance, $x=42$ yields $p=1847$, whereas $y=43$ gives the same prime. Conway and Guy [1] point out that Formula (3.2) represents primes for the consecutive numbers $n=1,2,\ldots,p-1$ provided that $1-4p$ is one of the Heegner numbers [10]:

$$\{-1,-2,-3,-7,-11,-19,-43,-67,-163\}.$$

The determination of these numbers is known as Gauss' class number problem. Trying to determine whether there was a tenth number was a notorious problem for a long time. Heegner [4] published a proof that the list of nine was complete, but there was considerable doubt about the validity of the proof until Stark [11] showed that the proof was essentially correct. The Heegner numbers have a number of arithmetical links with algebraic integers and transcendental numbers.

References

1. J.H. Conway and R.K. Guy, *The Book of Numbers*. New York: Springer-Verlag, 1996.
2. Marcus du Sautoy, *The Music of the Primes: Searching to Solve the Greatest Mystery in Mathematics*. New York: Harper Collins, 2003.
3. L. Euler, *Opera Omnia*. Leipzig: Teubner, 1911.
4. K. Heegner, Diophantische Analysis und Modulfunktionen, *Mathematische Zeitschrift*. **56**, (1952): 227-253.
5. J.V. Leyendekkers, J.M. Rybak & A.G. Shannon, Analysis of Diophantine Properties Using Modular Rings with Four and Six Classes. *Notes on Number Theory & Discrete Mathematics*. **3 (2)** (1997): 61-74.
6. J.V. Leyendekkers & A.G. Shannon, The Analysis of Twin Primes within Z_6. *Notes on Number Theory & Discrete Mathematics*. **7(4)** (2001): 115-124.
7. J.V. Leyendekkers & A.G. Shannon, Some Characteristics of Primes within Modular Rings. *Notes on Number Theory & Discrete Mathematics*. **9(3)** (2003):49-58.
8. J.V. Leyendekkers & A.G. Shannon, The Row Structure of Squares in Modular Rings. *International Journal of Mathematical Education in Science & Technology*. **35(6)** (2004): 932-936.
9. Hans Riesel. *Prime Numbers and Computer Methods for Factorization. Progress in Mathematics Volume 126*. Boston: Birkhäuser, 1994.
10. N.J.A. Sloane, Sequences A003173/M087, *The On-Line Encyclopedia of Integer Sequences*. http://www.research.att.com/ njas/sequences/.
11. H.M. Stark, On Complex Quadratic Fields with Class Number Equal to One. *Transactions of the American Mathematical Society*. **122**, (1966): 112-119.

AMS Classification Numbers: 11A41, 11A07