PACIFIC JOURNAL OF MATHEMATICS
Vol. 37, No. 3, 1971

PRIME GENERATORS WITH PARABOLIC LIMITS

JOHN HARRIS AND OLGA HIGGINS

The prime generating properties of the formula

$$F = \frac{AX^2 + ABXY + CY^2}{(A, Y)}\ , \quad (X, Y) = 1$$

are developed by way of three theorems. Theorem I is a prime test for F, Theorem II will factor a composite F, and Theorem III establishes parabolic limits; within these limits F is always prime.

In the 18th century Leonhard Euler and A. M. Legendre found several "prime generating" polynomials. Euler's famous formula $X^2 + X + 41$ takes prime values for every integral value of x from 0 to 39, and Legendre's formula $2x^2 + 29$ does almost as well, taking prime values for every integral value of x from 0 to 28. These and many other expressions that have been found since have coefficients of the form $[A, AB, C]$, with $B = 0$ or 1 and C a prime.

After numerous experiments with two variables we have chosen

$$F = \frac{AX^2 + ABXY + CY^2}{E}\ , \quad E = (A, Y), (X, Y) = 1$$

as our basic "prime generating" formula. The coefficients A, B and

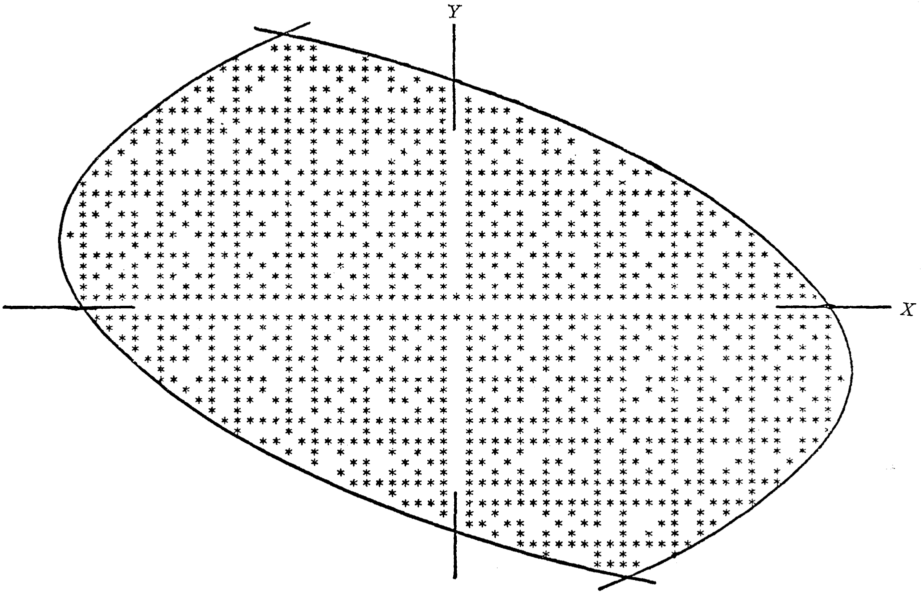

FIGURE 1

C are to be chosen from Table I, and then F is a function of the two variables X and Y. That this can be a very effective prime generator is shown by Fig. 1, where all of the dots represent primes; see Example 3. Figure 1 shows the typical dot pattern which is due to the requirement $(X, Y) = 1$. F is defined differently in the text by the definitions of § 2, but the mathematical result is the same as shown in the proof of Theorem III.

The three theorems presented in this paper answer some of the more interesting questions about our formula. Theorem I is a prime test that determines whether F is prime or composite. Theoretically it will test numbers of any size, see Example 1. Theorem II will factor a number found composite by Theorem I. Theorem III gives the prime generating limits of our formula; the parabolic limits inside of which there are no composite values of F. Fig. 1 shows how these limits are established by intersecting parabolas. The nature of F outside the limits is not shown in Fig. 1; there are primes, which could be shown by dots, and composites, which could be represented by some other symbol.

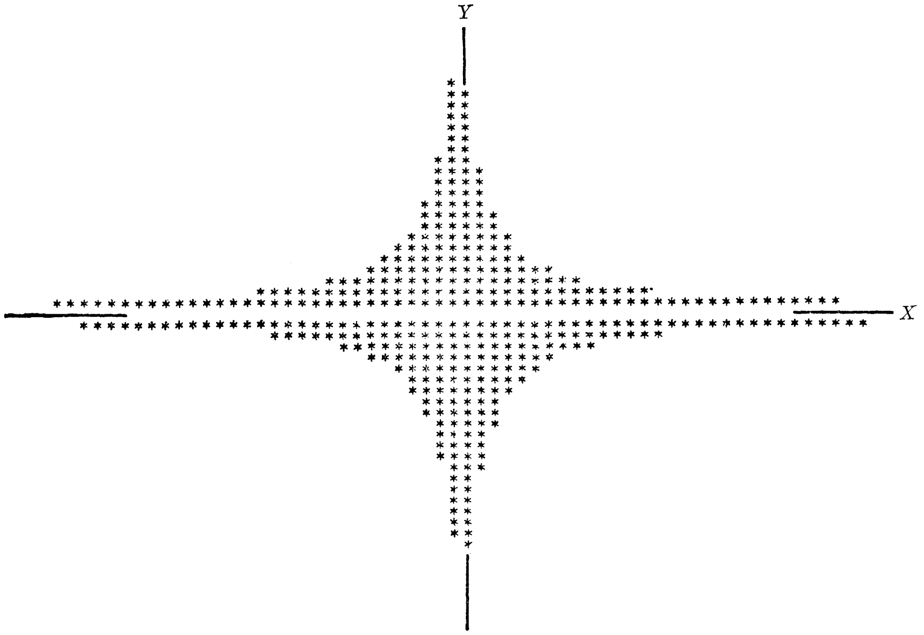

FIGURE 2

Example 4 and Fig. 2 present a function that is perhaps more in the spirit of Euler's original discovery; the function has prime values within the limits for consecutive integral values of both variables. In this case the limits are hyperbolas.

2. Definitions and two theorems. Let A, B and C be any integers subject to the following conditions: [See Table I.]

TABLE I

A list of coefficients for use with all three theorems:

Values of A and C when B = O:

$C = 2$:	$A = 1,3,5,11,15,21,29,35,39,51,65,95,105,165,231$.
$C = 3$:	$A = 2,10,14,26,34,70,110,154$.
$C = 5$:	$A = 2,6,14,26,38,42,66$.
$C = 7$:	$A = 6,10,30,66$.
$C = 11$:	$A = 2,30,42$.
$C = 13$:	$A = 6,10$.
$C = 17$:	$A = 6$.
$C = 19$:	$A = 10$.
$C = 29$:	$A = 2$.

Values of A and C when B = 1:

$C = 2$:	$A = 1,3,5$.
$C = 3$:	$A = 1,2,5,7$.
$C = 5$:	$A = 1,3,6,7,13,14,17$.
$C = 7$:	$A = 2,5,6,11,15,17,22,23$.
$C = 11$:	$A = 1,3,6,10,13,15,21,30,31,34,38,39,41$.
$C = 13$:	$A = 5,14,15,30,33,38,42,47$.
$C = 17$:	$A = 1,6,7,15,22,42,46,55,57,61,62,65$.
$C = 19$:	$A = 2,30,35,42,65,66,69,70$.
$C = 23$:	$A = 3,70,78,85,87,89$.
$C = 29$:	$A = 102,105,110,111$.
$C = 31$:	$A = 6,105,110,118,119$.
$C = 37$:	$A = 138,143,145$.
$C = 41$:	$A = 1,154,159,161$.
$C = 43$:	$A = 165$.
$C = 47$:	$A = 182,185$.
$C = 53$:	$A = 195,205,209$.
$C = 59$:	$A = 210,230,231$.
$C = 61$:	$A = 231,238$.
$C = 67$:	$A = 255,265$.
$C = 71$:	$A = 273$.
$C = 73$:	$A = 285,287$.
$C = 97$:	$A = 385$.
$C = 101$:	$A = 390,399$.
$C = 109$:	$A = 429$.
$C = 139$:	$A = 546$.
$C = 167$:	$A = 663,665$.
$C = 229$:	$A = 910$.
$C = 251$:	$A = 1001$.
$C = 277$:	$A = 1105$.

C1. $A > 0$, $B = 0$ or $B = 1$, C is a prime.

C2. AC has no square factors > 1.

C3. $4C - AB^2 > 2$.

C4. Every positive integral binary quadratic form with the discriminant $-D$ [see D1 below] must be equivalent to one of the forms $[A/e, AB, eC]$, where e is any positive divisor of A.

DEFINITIONS.

D1. Let $D = 4AC - A^2B^2$; then $D > 2$ by C1 and C3.

D2. Let E be a positive divisor of A.

D3. Let X and y be any two integers such that $(XA/E, Ey) = 1$ and $y \neq 0$.

D4. Let $F = (A/E)X^2 + ABXy + ECy^2$.

D5. Let $Y = Ey$, so $Y \neq 0$; and let $Z = 2AX + ABY$.

D6. Let I be any integer and let $N = -DI^2 + 2ZI + Y^2$.

THEOREM I. *F is a prime if and only if N is never a square when $I \neq 0$; this can be determined in a finite number of steps.*

THEOREM II. *When $N = n^2$ with $I \neq 0$, a proper divisor $M > 1$ of F can be found as follows: Let $L = AI$, $H = (n - BL - Y)/2$, $G = (H, L)$, $R = H/G$, $S = L/G$, $Q = (A, S)$, and then: $M = (AR^2 + ABRS + CS^2)/Q$.*

3. Outline of the proofs. First we show that $F > 1$, so F is either prime or composite; next, when F is composite, nonzero integers W and K are found such that N is a square when $I = KW$; finally, we prove Theorem II, so if N is a square with $I \neq 0$ then F must be composite. That only a finite number of values of I can make N positive or zero [and so possibly a square] follows from D1 and D6. When these facts are combined they prove Theorem I.

4. Preliminary Theory. [$F > 1$, $(F, A) = 1$, and the form of a divisor of F.]

The proof that $F > 1$: From D3, D4 and D5,

$$EF = AX^2 + ABXY + CY^2\,, \qquad (X, Y) = 1\,; \tag{1}$$

so $4AEF = (2AX + ABY)^2 + (4AC - A^2B^2)Y^2$, which reduces to

$$4F = (A/E)(2X + BY)^2 + (4C - AB^2)(Y^2/E)\,.$$

A/E and Y^2/E are positive integers and $4C - AB^2 > 2$ by C3, so $F > 0$, and if $F = 1$ then $4C - AB^2 = 3$ or 4. Since $C > 1$ by C1 we have $B = 1$, $Y^2/E = 1$, $Y^2 = 1$, $E = 1$, $4C - A = 4 - A(2X \pm 1)^2 = 3$ or 4; then $A = 1$ and $4C - A = 3$ or 4, which is impossible. Hence $F > 1$.

The proof that $(F, A) = 1$: Let a prime p divide both F and A. Then $p \mid Y$ by C2 and (1), which implies $X \neq 0$ and $p \nmid X$ by $(X, Y) = 1$. $(A/E, y) = 1$ from D3 so $(A, Y) = E$ and $p \mid E$; but this leads to the impossible conclusion that p^2 divides every term of (1) except AX^2 [see C2]. Hence $(F, A) = 1$.

Definition of P. Let P be any prime divisor of F.

Then since $P|EF$ which is properly represented by $[A, AB, C]$ as shown by (1), a form with the discriminant $-D$, it follows by Lagrange's well known theorem that P can also be represented by a form with the discriminant $-D$. Then the fact that equivalent forms represent the same numbers, and C4, combine to show that P can be represented by $[A/J, AB, JC]$, where J is a positive divisor of A. Integers u and W can therefore be found such that

(2) $P = (A/J)u^2 + ABuW + JCW^2$. [Compare to D4.]

Then we also have:

(3) $P = (A/J)(-u - BJW)^2 + AB(-u - BJW)W + JCW^2$,

since by eliminating P between (2) and (3) we arrive at an identity. Also an identity: $(AX^2 + ABXY + CY^2)JW^2 - (A/Ju^2 + ABuW + JCW^2)Y^2 = (A/J)(JWX - uY)(JWX + uY + BJWY)$, so from (1) and (2):

(4) $EFJW^2 - PY^2 = (A/J)(JWX - uY)(JWX + uY + BJWY)$,

where A/J is integral. It follows from $(F, A) = 1$ that $(P, A) = 1$, so from (4): P divides either $JWX - uY$ or $JWX + uY + BJWY$, or both. If P divides $JWX - uY$, let $U = u$; if not, let $U = -u - BJW$. P divides $JWX - UY$ in both cases, so let

(5) $$K = \frac{JWX - UY}{P} ;$$

then K is always integral. By (2) or (3),

(6) $P = (A/J)U^2 + ABUW + JCW^2$.

5. The proof that a nonzero value of I, I = KW, makes N a square when F is composite. Let F be composite. Then $X \neq 0$, since if $X = 0$ we have $Y^2 = 1$, $y^2 = E = 1$, $F = C$. Also, $W \neq 0$ by (6), $(P, A) = 1$, and $P \neq 1$. [$P \neq 1$ because it is prime.] Finally, $(U, JW) = 1$, because if U and J have a common prime divisor it must divide both P [by (6)] and A, contradicting $(P, A) = 1$; while if a prime divides both U and W, its square divides the prime P by (6).

Now suppose that $K = 0$; then $JWX = UY$ by (5), where

$JWXY \neq 0$; hence $U \neq 0$. Then $(X, Y) = 1$, $(U, JW) = 1$ and $JWX = UY$ shows that $X|U$ and $U|X$, so $X = U$ and $Y = JW$ or $X = -U$ and $Y = -JW$. In both cases, $EF = JP$ by (1) and (6), and since $(FP, EJ) = 1$ [E and J divide A], we conclude that $F = P$, a prime. Hence $KW \neq 0$ when F is composite.

Let $I = KW$ with F composite, so $I \neq 0$; eliminating P between (5) and (6) and multiplying by $(4AK^2)/J$, we get:

$$(2AKU/J)^2 + 2(2AKU/J)ABI + 4ACI^2 = 4AXI - 4AKUY/J\,,$$

which reduces to

$$N = (2AKU/J + ABI + Y)^2\,, \tag{7}$$

by D1, D5 and D6. Since $J|A$, N is a square.

6. The proof of Theorem I and Theorem II. From $N = n^2$ and D6:

$$n^2 = -DI^2 + 2ZI + Y^2\,. \tag{8}$$

New Definitions.

D7. $L = AI.$

D8. $H = (n - BL - Y)/2,$ $\quad h = (-n - BL - Y)/2.$

D9. $G = (H, L),$ $\quad g = (h, L).$

D10. $R = H/G,$ $\quad r = h/g.$

D11. $S = L/G,$ $\quad s = L/g.$

D12. $Q = (A, S),$ $\quad q = (A, s).$

D13. $M = (AR^2 + ABRS + CS^2)/Q,$ $\quad m = (Ar^2 + ABrs + Cs^2)/q.$

Let n be integral with $N = n^2$ and with $I \neq 0$. Then $L \neq 0$, $S \neq 0$ and $s \neq 0$. $2H$ and $2h$ are integral by D8, they have an even product $(2H)(2h) = 4L(CI - X)$ by D8, D7; and (8), D1 and D5. Also, $2H - 2h = 2n$ by D8, so $2H$ and $2h$ have an even difference and are both odd or both even; with an even product, they must be even. *Hence H and h are integral.* $Hh = L(CI - X)$, so *L divides Hh.* From (1), D1 and D5,

$$4AEF = Z^2 + DY^2\,, \tag{9}$$

and there are similar formulas for M and m:

$$4AQM = (2AR + ABS)^2 + DS^2\,,\quad 4Aqm = (2Ar + ABs)^2 + Ds^2\,. \tag{10}$$

$2R + BS = (2H + BL)/G = (n - Y)/G$ by D10, D11 and D8, and similarly, $2r + Bs = (-n - Y)/g$. $S = AI/G$ and $s = AI/g$, so from (10), $4AQMG^2 = A^2([n - Y]^2 + DI^2)$ and $4Aqmg^2 = A^2([-n - Y]^2 +$

DI^2). Hence, $16QqMmG^2g^2 = A^2(4Z^2I^2 + 4DI^2Y^2) = 4A^2I^2(4AEF)$ by (8) and (9), so

$$\left(\frac{Gg}{L}\right)^2 QqMm = AEF . \tag{11}$$

$L \mid Hh$; $G = (H, L)$; and $g = (h, L)$. Let p be a prime divisor of L, and let the symbol "$p(a)$" represent the highest power of p which divides a. If $p(H) \geqq p(L)$ or $p(h) \geqq p(L)$, then $p(G) = p(L)$ or $p(g) = p(L)$ and $p(Gg) \geqq p(L)$. In the remaining case, both $p(H)$ and $p(h)$ are less than $p(L)$, so $p(G) = p(H)$ and $p(g) = p(h)$, and then $p(Gg) = p(Hh) \geqq p(L)$. In all cases the highest power of P which divides L also divides Gg, and so *L divides Gg*.

The proof that M is a proper divisor of F. In view of (11) and the last result, we need only show that $M > 1$, $m > 1$, and $(Mm, AE) = 1$. From D9, D10 and D11, we have $(R, S) = 1$. Compare this to $(X, Y) = 1$; $QM = AR^2 + ABRS + CS^2$ to (1); and $Q = (A, S)$ to $E = (A, Y)$. Also note $S \neq 0$ and $Y \neq 0$; clearly the substitution of R, S and Q for X, Y and E converts F into M. In fact, M is one of the numbers F, but not the one of which M is a divisor. It follows that $M > 1$, $(M, A) = 1$, and by similar reasoning, $m > 1$ and $(m, A) = 1$. Since $E \mid A$, we have $(Mm, AE) = 1$, and the proof that M is a proper divisor of F is complete. This proves Theorem II. The proof of Theorem *I* is now also complete by the reasoning given in "outline of the proofs".

The number of values of I for which N needs to be tested is approximately $(4\sqrt{AEF})/D$, so $D/\sqrt{AE}$ should be large for an efficient test. Of all the values given in Table *I*, $A = 210$, $B = 1$, $C = 59$, $E = 1$ gives the largest, with $D/\sqrt{AE} = 376$.

EXAMPLE 1. Let $A = B = 1$, $C = 41$. Then $E = 1$, $Y = y$, and $F = X^2 + XY + 41Y^2$. Let $X = 1000$ and $Y = 1$. Then

$$F = 1,001,041, \text{ and } N = -163I^2 + 4002I + 1 .$$

N is negative for negative I and for $I > 24$, so we test the 24 values of N given by $I = 1, 2, 3, \cdots, 24$. We get $N = 3840$, 7353, 10540, etc., and find no squares, so F is a prime. [See Theorem *I*.]

EXAMPLE 2. Let $A = 6$, $B = 1$, $C = 31$; these values can be found in Table I. Let $E = 2$, $X = 423$, $y = 19$, then $(XA/E, Ey) = 1$ as required by D3, and $F = 3(423)^2 + 6(423)(19) + 62(19)^2 = 607391$; and F is composite, because for $I = 3$ we find $N = (164)^2$. By Theorem

II we now have: $n = 164$, $L = 18$, $H = 54$, $G = 18$, $R = 3$, $S = 1$, $Q = 1$, and $M = 103$. The factors of F are 103 and 5897.

7. Theorem III and its proof.

THEOREM III. *Define A, B, C and D as before, let X and Y be any two relatively prime integers such that the following limits are satisfied:*

$$D - Y^2 > |4AX + 2ABY| ; \tag{12}$$

and let

$$F = \frac{AX^2 + ABXY + CY^2}{(A, Y)} .$$

Then F is a prime when $Y \neq 0$.

Proof. Let $E = (A, Y)$ and let $y = Y/E$, then from $(A/E, E) = 1$, $(A/E, y) = 1$, and $(X, Ey) = 1$, we find $(XA/E, Ey) = 1$ as in D3. Also, $F = (A/E)X^2 + ABXy + ECy^2$, and the preliminary requirements of Theorem I are satisfied. By D5 and (12), $D - Y^2 < 2|Z|$. Then by D6, N is negative for $I = 1$ and for $I = -1$, and since N is positive for $I = 0$ and is of the second degree in I, it follows that N is negative for all integral values of I except $I = 0$, for otherwise the equation $N = 0$ would have more than two roots for real values of I. Hence F is prime by Theorem I.

EXAMPLE 3. Let $A = 6$, $B = 1$, and $C = 31$. Then from Theorem III: $F = (6X^2 + 6XY + 31Y^2)/(6, Y)$ is a prime when $(X, Y) = 1$ and $Y \neq 0$ and:

$$31 - \frac{(Y+6)^2}{24} > X > \frac{(Y-6)^2}{24} - 31 . \tag{13}$$

[(13) follows in a simple way from (12).] It can be seen from (13) that the limits are parabolas. There are 309 different values of F within the limits (13); see Fig. 1, where each prime is represented by four symmetrically placed points (X, Y), corresponding to the four representations of a prime F by $[6/E, 6, 31\ E]$. [$F = 59$ is an exception, since 59 divides D.] Every lattice point within the limits (13) and with $(X, Y) = 1$ is marked, and the parabolas found by placing equals signs in (13) are shown in the figure.

EXAMPLE 4. Replace X by $XY + 1$ in all the formulas of Example 3. The result can be seen in Fig. 2; the limits have become hyperbolas, and every lattice point with $Y \neq 0$ and within the limits corresponds to a prime. Some of the primes of Fig. 1 are lost by the transformation, but 150 distinct primes remain.

Reference

A number of references are given in Dickson's "History of the Theory of Numbers", Vol. I, Pages 420, 421.

Received March 7, 1968.