Bollettino dei Docenti di Matematica del Canton Ticino, 31 (1995), 33-38
(in Italian)

Prime numbers and quadratic polynomials

GIORGIO T. BAGNI

Summary. Some nonconstant polynomials with a finite string of prime values are known; in this paper, some polynomials of this kind are described, starting from Euler's example (1772) $P(x) = x^2+x+41$: other quadratic polynomials with prime values were studied, and their properties were related to properties of quadratic fields; in this paper, some quadratic polynomials with prime values are described and studied.

Lisez Euler,
c'est notre maître à tous!
Pierre Simon de Laplace

Several mathematicians studied polynomials assuming primes values, from XVIII to XX century. In this paper, polynomials $P(x)$ in the one indeterminate x with integral coefficients are examined, such that $P(\alpha)$ is a prime if α is an integer satisfying some conditions.

First of all, let us underline that polynomials of this kind cannot assume prime values for every integer α: it is possible to prove that if $P(x)$ is a nonconstant polynomial with integral coefficients in the one indeterminate x, then there exists infinitely many integers x such that the value $|P(x)|$ is *not* a prime number ([4], p. 136). Other negative results, for polynomials in n indeterminates and with complex coefficients, and for rational functions, were showed in the XX century (Reiner, 1943, Buck, 1946) ([4], pp. 136-137).

In many cases, however, it is possible to find polynomials with "a long string of prime values" (according to Ribenboim's description, in [4], p. 137).

Let us consider the set of prime numbers:

41, 41+2, 41+2+4, 41+2+4+6, 41+2+4+6+8, ...

It consists of 40 elements and it can be written in the form:

$$\{m(h)\in \mathbf{Z}^+: m(h) = h^2+h+41) \wedge h\in \mathbf{Z} \wedge 0\leq h\leq 39\}$$

and in the form: {41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601}. Note that $m(40) = 41+40\cdot(40+1)$ is composite.

This set of prime numbers can be obtained from a famous Euler's quadratic polynomial with integral coefficients: in 1772, Leonhard Euler (1707-1783) noted that the values of $P(x) = x^2+x+41$, for x integer, $0 \le x \le 39$, are primes.

It is interesting to investigate about polynomials like Euler's one: are there other polynomials of the form x^2+x+q, where q is a prime number, with prime values for $x = 0, 1, ..., q-2$? Are there other quadratic polynomials, with integral coefficients, with a "long string" of prime values?

First of all, let us consider polynomials of the form x^2+x+q, where q is a prime number (41, as in Euler's example, but also a prime number different from 41); Paulo Ribenboim, in *The Book of Prime Number Record* [4], writes:

"For polynomials of the form x^2+x+q, where q is a prime number, I note the interesting equivalent properties:

(1) $q = 2, 3, 5, 11, 17,$ o 41.

(2) x^2+x+q assumes prime values for $x = 0, 1, ..., q-2$.

(3) The field $Q\left(\sqrt{1-4q}\right)$ of all algebraic numbers of the form $r+s\sqrt{1-4q}$ (where r, s are rational numbers) has class number 1" ([4], p. 137).

Many mathematicians worked to determine all the primes q for which the field $Q\left(\sqrt{1-4q}\right)$ has class number 1. In 1801, Gauss (1777-1855) proved that if $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$, then the field $Q\left(\sqrt{-d}\right)$ has class number 1. Gauss himself conjectured that there are no other values of d for which the field $Q\left(\sqrt{-d}\right)$ has class number 1 ([3], pp. 204-230, [4], pp. 964-968); this was proved in XX century (Heilbronn and Linfoot, 1934; Heegner, Baker and Stark, 1952-1966) ([4], pp. 138-139). It is possible to show that the values $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ yield to the six values $q = 2, 3, 5, 11, 17, 41$.

The study mentioned above does not consider all quadratic polynomials with integer coefficients; the research about *other* quadratic polynomials is related to the study of imaginary quadratic fields (Dirichlet, 1839-1840; Baker, 1969-1971; Montgomery e Weiberger 1974; Stark, 1975). Ribenboim writes:

"Consider the polynomials:

(I) $f(x) = 2x^2+p$

(II) $f(x) = 2x^2+2x+(p+1)/2$ where $p \equiv 1 \pmod 4$

(III) $f(x) = px^2+px+(p+q)/2$ where $p < q$ and $pq \equiv 3 \pmod 4$.

(I) The only polynomials of type I are $2x^2+p$, with $p = 3, 5, 11, 29$, and they assume prime values $x = 0, 1, ..., p-1$.

(II) The only polynomials of type II are $2x^2+2x+n$, with $n = 3, 7, 19$, and they assume prime values $x = 0, 1, ..., n-2$.

(III) The only polynomials of type III are px^2+px+n, with (p, n) equal to the following pairs: (3, 2), (3, 5), (3, 11), (3, 23), (5, 3), (5, 7), (5, 13), (7, 5), (7, 17), (11, 7), (13, 11); they assume prime values for $x = 0, ... n-2$" ([4], p. 142).

In the last few years, deep studies by Mollin and Williams (1990), by Louboutin (1990 and 1991) and by Mollin (1994) improved our knowledge of quadratic polynomials. These researches are based upon thecniques of higher mathematics and they are not didactically very important; it can be interesting to consider the problem from an elementary point of wiew [Bagni, 1993].

If we consider polynomials of the kind $Q_{a,\ p}(x) = ah^2+ah+p$, and the sets expressed by [1]:

$$I(a; p) = \{m(h)\in \mathbf{N}: m(h) = ah^2+ah+p \wedge h\in \mathbf{N} \wedge 0\leq h\leq p-2\}$$

(without considering the question about the class number of quadratic imaginary fields), we can note that for some pairs $(a; p)$ not given by Ribenboim the set $I(a; p)$ consists only of prime numbers.

Some results about sets $I(a; p)$ can be proved with simple thecniques ([1], for example, it is easy to show that if $p|a$, then the set $I(a; p)$ does *not* consist only of prime numbers).

Sets $I(a; 2) = \{2\}$ consist of only one element (prime). Sets $I(a; 3)$ consist of two elements and it is immediate to prove the trivial result:

Proposition 1. If q is a prime number, $q\geq 5$, then the set $I\left(\frac{q-3}{2},3\right) = \{3; q\}$ consists only of prime numbers. ν

So for every q prime, $q\geq 5$, it is possible to find a set $I\left(\frac{q-3}{2},3\right) = \{3; q\}$ which consists only of prime numbers. If p is a prime and $p>3$, the research of sets $I(a, p)$ consisting only of prime numbers needs computer's aid [5].

$I(a; p)$ has been checked for p prime, $p\leq 100$ and for $a\leq 100000$ (for $p>41$: $a\leq 20000$); the following sets consist only of prime numbers:

- $I(a; 5)$ for the following values of a (let us list 65 sets for $a\leq 1000$):

1 3 4 7 9 16 21 24 37 42 46 51 63 66 73 79 81 84
123 136 156 184 196 198 217 219 228 241 247 268 282
301 318 339 367 373 429 436 438 451 483 514 522 612
627 646 651 702 709 711 714 724 753 763 774 781 802
847 858 871 898 921 931 973 997

For:	$1 \le a \le 10000$: 260 val.	$50000 \le a \le 60000$:	123 val.
	$10000 \le a \le 20000$: 163 val.	$60000 \le a \le 70000$:	107 val.
	$20000 \le a \le 30000$: 145 val.	$70000 \le a \le 80000$:	117 val.
	$30000 \le a \le 40000$: 139 val.	$80000 \le a \le 90000$:	104 val.
	$40000 \le a \le 50000$: 126 val.	$90000 \le a \le 100000$:	106 val.

- I(a; 7) for the following values of a (let us list 12 sets for $a \le 1000$):

  2 5 11 36 71 165 282 296 656 830 902 986

For:	$1 \le a \le 10000$: 40 val.	$50000 \le a \le 60000$:	9 val.
	$10000 \le a \le 20000$: 16 val.	$60000 \le a \le 70000$:	9 val.
	$20000 \le a \le 30000$: 13 val.	$70000 \le a \le 80000$:	5 val.
	$30000 \le a \le 40000$: 11 val.	$80000 \le a \le 90000$:	6 val.
	$40000 \le a \le 50000$: 11 val.	$90000 \le a \le 100000$:	9 val.

- I(a; 11) for the following values of a (let us list 7 sets for $a \le 100000$):

  1 3 13 951 16960 38248 50676 (then: 140335; 174910)

Ex.: I(16960; 11) = {11, 33931, 101771, 203531, 339211, 508811, 712331, 949771, 1221131, 1526411}
I(38248; 11) = {11, 76507, 229499, 458987, 764971, 1147451, 1606427, 2141899, 2753867, 3442331}
I(50676; 11) = {11, 101363, 304067, 608123, 1013531, 1520291, 2128403, 2837867, 3648683, 4560851}
I(140335; 11) = {11, 280681, 842021, 1684031, 2806711, 4210061, 5894081, 7858771, 10104131, 12630161}
I(174910; 11) = {{11, 349831, 1049471, 2098931, 3498211, 5247311, 7346231, 9794971, 12593531, 15741911}

- For p prime, $13 \le p < 41$: I(5; 13), I(1; 17), I(7; 17), I(2; 19), I(3; 23) and I(1; 41) consist only of prime numbers (we checked $a \le 100000$).

Then the number of sets I(a; p) consisting only of prime numbers is rather high for p = 5 (1390, a≤100000) and for p = 7 (129, a≤100000); we have only 7 sets for p = 11, 1 set for p = 13, 2 sets for p = 17, 1 set for p = 19 and 1 set for p = 23. For 23<p<41 no I(a; p) consisting only of prime numbers were found (a≤ 100000); for p = 41 we found only Euler's set (a≤100000). For 41<p<100 no I(a; p) consisting only of prime numbers were found (a≤20000).

Let us study sets I(a; p) in the form (by writing: $h = p-j-2$):

$$\mathrm{I}(a;p) = \{m(j)\in\mathbf{N}: m(j) = ap^2-(2aj+3a-1)p+a(j+1)(j+2) \wedge j\in\mathbf{N} \wedge 0\le j\le p-2\}$$

Proposition 2. If $a = 2(2j+3)$, then $m(j)\in$ I(a; p) is *not* a prime number, for all $j\in\mathbf{N} \wedge 0\le j<p-2$.

Proof. Let us consider $\Delta(a; j) = a^2-2a(2j+3)+1 = a(a-4j-6)+1$ referred to $ap^2-(2aj+3a-1)p+a(j+1)(j+2) = m(j)$. If $a = 2(2j+3)$, then $\Delta(a; j) = 1$; so:

$$m(j) = (2p-2j-3)\cdot[(2j+3)p-2(j+1)(j+2)]$$

Let us show that neither $2p-2j-3$ is 1 nor $(2j+3)p-2(j+1)(j+2)$ is 1:

$2p-2j-3 = 1 \;\Rightarrow\; j = p-2$ and this is impossible, being $j\in\mathbf{N} \wedge 0\le j<p-2$;

$(2j+3)p-2(j+1)(j+2) = 1 \;\Rightarrow\; j = \dfrac{p-3\pm\sqrt{p^2-1}}{2}$, impossible, being $j\in\mathbf{N}$.

This explains why I(6; p) does *not* consist only of prime numbers.

Proposition 3. If there exists $b\in\mathbf{N}$ such that: $a^2-2a(2j+3)+1 = b^2$ or, (as it is equivalent): $a = 2j+3+\sqrt{(2j+3)^2+b^2-1}$, or: $j = \dfrac{a^2-6a+1-b^2}{4a}$, with $a\in\mathbf{N}$, $0\le j<p-2$, then the set:

$$\mathrm{I}(a;p) = \{m(j)\in\mathbf{N}: m(j) = ap^2-(2aj+3a-1)p+a(j+1)(j+2) \wedge j\in\mathbf{N} \wedge 0\le j\le p-2\}$$

does *not* consist only of prime numbers.

Proof. If $\Delta(a; j) = a^2-2a(2j+3)+1 = b^2$ it is possible to write:

$$m(j) = a\cdot\left(p-\frac{2aj+3a-1+b}{2a}\right)\cdot\left(p-\frac{2aj+3a-1-b}{2a}\right)$$

$$j=\frac{a^2-6a+1-b^2}{4a}\in\mathbf{N}\quad\Rightarrow\quad\frac{a}{4}-\frac{3}{2}+\frac{(1+b)(1-b)}{4a}\in\mathbf{N}$$

and factors of a are factors of $(1+b)(1-b)$; so:

$m(j)=a\cdot\left(p-j-\frac{3}{2}+\frac{1+b}{2a}\right)\cdot\left(p-j-\frac{3}{2}+\frac{1-b}{2a}\right)$ is a product of integers.

Let us show that:

neither $p-\frac{2aj+3a-1+b}{2a}$ is 1,
nor $a\cdot\left(p-\frac{2aj+3a-1+b}{2a}\right)$ is 1,
nor $p-\frac{2aj+3a-1-b}{2a}$ is 1,
nor $a\cdot\left(p-\frac{2aj+3a-1-b}{2a}\right)$ is 1.

Let us write: $j=p-2-q\ \wedge\ q\in\mathbf{N}\ \wedge\ 0<q\le p-2$.

- If $p-\frac{2aj+3a-1+b}{2a}=1$, it sholud be:
  $2ap-2aj-5a+1-\sqrt{a^2-2a(2j+3)+1}=0$
  $\sqrt{a^2+2a(2q-2p+1)+1}=2aq-a+1$
  $aq^2-aq+p-1=0\quad\Rightarrow\quad q=\frac{1}{2}\pm\frac{\sqrt{a^2-4ap+4a}}{2a}$
  and being $q\in\mathbf{N}\ \wedge\ 0<q\le p-2$: $a^2-4a(p-1)=k^2a^2\ \wedge\ k\in\mathbf{N}$
  $a(1-k^2)=4(p-1)$ and this is impossible being $p\in\mathbf{N}$ prime.

- If $a\cdot\left(p-\frac{2aj+3a-1+b}{2a}\right)=1$, it sholud be:
  $2ap-2aj-3a-1-\sqrt{a^2-2a(2j+3)+1}=0$
  $\sqrt{a^2+2a(2q-2p+1)+1}=2aq+a-1$
  $aq^2+(a-2)q+p-1=0\quad\Rightarrow\quad q=\frac{2-a\pm\sqrt{a^2-4ap+4}}{2a}$

for $p>1$, it is: $\frac{2-a-\sqrt{a^2-4ap+4}}{2a} < \frac{2-a+\sqrt{a^2-4ap+4}}{2a} < 0$
and this is impossible, being $q \in \mathbf{N}$.

- If $p-\frac{2aj+3a-1-b}{2a} = 1$, it sholud be:
  $2ap-2aj-5a+1+\sqrt{a^2-2a(2j+3)+1} = 0$
  $a(2q-1)+1+\sqrt{a^2-2a(2j+3)+1} = 0$ and this is impossible.

- If $a \cdot \left(p-\frac{2aj+3a-1-b}{2a} \right) = 1$, it sholud be:
  $2ap-2aj-3a-1+\sqrt{a^2-2a(2j+3)+1} = 0$
  $\sqrt{a^2+2a(2q-2p+1)+1} = 1-a(2q+1)$
  and this is impossible, being $q \in \mathbf{N} \wedge 0<q\leq p-2$.

As application of proposition 3, let us consider the case $a = 30$ and the following three choices, satisfying hypotheses of the proposition:

(α)	$a = 30$	$j = 3$	$b = 19$
(β)	$a = 30$	$j = 3$	$b = 11$
(γ)	$a = 30$	$j = 6$	$b = 1$

In the case (α), $m(j)$ can be factorized in the following way:

$$m(j) = 30\left(p-\frac{24\cdot 6}{5\cdot 6} \right)\left(p-\frac{25\cdot 5}{5\cdot 6} \right) = 30\left(p-\frac{24}{5} \right)\left(p-\frac{25}{6} \right) = (5p-24)(6p-25)$$
$$m(j) = 30\left(p-\frac{20\cdot 10}{3\cdot 10} \right)\left(p-\frac{21\cdot 9}{3\cdot 10} \right) = 30\left(p-\frac{20}{3} \right)\left(p-\frac{63}{10} \right) = (3p-20)(10p-63)$$

In the case (γ), $m(j)$ can be factorized in the following way:

$$m(j) = 30\left(p-\frac{15\cdot 15}{2\cdot 15} \right)\left(p-\frac{16\cdot 14}{2\cdot 15} \right) = 30\left(p-\frac{15}{2} \right)\left(p-\frac{112}{15} \right) = (2p-15)(15p-112)$$

The number of pairs (a, j) such that $a^2-2a(2j+3)+1 = b^2$, with $b \in \mathbf{N}$, is equal to the number of possibilities of writing two factors of a in the denominators into the brackets, being these denominators relatively prime ([1], p. 172).

It is important to underline that all the results above given are obtained by elementary thecniques.

The author wishes to express his warmest thanks to Professor Giulio Cesare Barozzi, to Professor Bruno D'Amore and to Professor Piero Plazzi, University of Bologna; thanks to Matteo Di Pieri, Sergio Serena and Alvise Spanò for computational controls.

Computational controls. Using the program *Mathematica* (for example, it is possible to consider I(a, 5) for $1 \le a \le 100000$):

```
i[{a_,p_}]:=Table[a h^2 + a h + p, {h,0,p-2}]
ctrl[a_,p_]:=Apply[And,PrimeQ[i[{a,p}]]]
Table[{ctrl[a,5], a, 5}, {a,1,100000}]
Select[%,(First[#]==True)&]
Map[i, Map[Rest, %]]
```

An Assembler source (Motorola MC68020+) is:

```
                                        ; Input:  d0.l=a(max)
                                        ;         d1.w=p
          movem.w     d0-d7/a0-a6,-(a7)
          btst        #0,d1
          beq.b       Bye
          lea         Tabella(pc),a0
          move.w      d1,a1               ; a1=p
          move.w      d1,a2
          subq.w      #2,a2               ; a2=h=p-2
          move.w      #2,a4
MainLoop: move.l      a2,d2               ; d2.w=h
Loop1:    move.l      d2,d3
          addq.l      #1,d3
          mulu.w      d2,d3
          mulu.l      d0,d3
          add.l       a1,d3               ; d3.l=n=a(h(h+1))+p
          cmp.l       a4,d3
          beq.b       nPrimo
          move.l      d3,a3
          move.l      d3,d7
          lsr.l       #2,d7
          addq.l      #1,d7
SqrtLp:   move.l      d7,d4               ; Newton
          move.l      d3,d7
          divul.l     d4,d5:d7
          add.l       d4,d7
          lsr.l       #1,d7
```

```
          cmp.l       d4,d7
          blo.b       SqrtLp
          moveq       #3,d5
          moveq       #3,d1
          moveq       #5+1,d3
          bra.b       dCheck
Loop2:    dbf         d1,Dec5
          moveq       #3-1,d1
          dbf         d3,dInc
          moveq       #5-1,d3
          bra.b       dInc
Dec5:     dbf         d3,Div
          moveq       #5-1,d3
          bra.b       dInc
Div:      move.l      a3,d7
          divu.w      d5,d7             ; d7lo.w=n/d,hi.w=n-dq
          swap        d7
          tst.w       d7                ; d7lo.w=0?
          beq.b       aDec
dInc:     addq.w      #2,d5
dCheck:   cmp.w       d4,d5
          bls.b       Loop2
nPrimo:   dbf         d2,Loop1
          move.l      d0,(a0)+          ; save a in RAM
aDec:     subq.l      #1,d0
          bhi.b       MainLoop
          rts
          cnop        0,8
Tabella   blk.b       1024
          end
```

Bibliography

[1] **G.T. Bagni**, *Alla ricerca di numeri primi*, in: "La matematica e la sua didattica", n. 2/1993, pp. 166-174, Pitagora, Bologna 1993.

[2] **G.H. Hardy & E.M. Wright**, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford 1938 (5th edition, 1979).

[3] **M. Kline**, *Mathematical thought from Ancient to Modern Times*, I, New York, 1972.

[4] **P. Ribenboim**, *The Book of Prime Number Records*, Springer-Verlag, New York 1980 (2nd edition, 1989).

[5] **R.S. Varga**, *Scientific Computation on Mathematical Problems and Conjectures*, SIAM, Philadelphia, Pennsylvania 1990.