When Can $(((X^2 - P)^2 - Q)^2 - R)^2 - S^2$ Split into Linear Factors?

Andrew Bremner

CONTENTS

We discover two infinite families of integers (P, Q, R, S) such that the polynomial $(((X^2 - P)^2 - Q)^2 - R)^2 - S^2$ factors into linear factors.

1. INTRODUCTION

The identity

$$((X^2 - 85)^2 - 4176)^2 - 2880^2 = (X^2 - 1^2)(X^2 - 7^2)(X^2 - 11^2)(X^2 - 13^2)$$

is given in [Crandall 96, p. 109], with a similar additional example

$$((X^2 - 377)^2 - 73504)^2 - 50400^2 = (X^2 - 5^2)(X^2 - 15^2)(X^2 - 23^2)(X^2 - 27^2)$$

in [Crandall and Pomerance 01], allowing the product of eight integers to be evaluated using three squaring and three subtraction operations. Such identities with k nested squares would give rise to 2^k integers of type $X \pm a_i$, for integers a_i, whose product therefore may be evaluated using k squaring and k subtraction operations; and such formulas could have useful consequence for the fast computation of factorials with impact in factorization theory; see [Dilcher 00] and also [Crandall 96, Crandall et al. 97] for a more general discussion of factorial evaluation.

It is straightforward to parameterize all such identities when $k = 3$. It is observed in [Dilcher 00, Section 2] that if $n = a_1^2 + b_1^2 = a_2^2 + b_2^2$, then

$$\left(\left(x^2 - \frac{n}{2}\right)^2 - \left(\frac{n^2}{4} - \frac{a_1^2 b_1^2 + a_2^2 b_2^2}{2}\right)\right)^2 - \left(\frac{a_1^2 b_1^2 - a_2^2 b_2^2}{2}\right)^2 = \left(x^2 - a_1^2\right)\left(x^2 - b_1^2\right)\left(x^2 - a_2^2\right)\left(x^2 - b_2^2\right).$$

2000 AMS Subject Classification: Primary 11D41; Secondary 11G05, 11G35, 11Y50

Keywords: Nested squares, elliptic curve

1058-6458/2008 $0.50 per page
Experimental Mathematics **17**:4, page 385

Indeed, this provides all parameterizations for $k = 3$. Suppose that

$$\begin{aligned}&\big((X^2-P)^2-Q\big)^2-R^2 \qquad (1\text{–}1)\\ &\quad=(X^2-A^2)(X^2-B^2)(X^2-C^2)(X^2-D^2).\end{aligned}$$

The factorization resulting from replacing (P,Q,R) by (a^2P,a^4Q,a^8R) is equivalent to replacing X by X/a, so we regard the two corresponding identities as equivalent. Now, (1–1) requires

$$\begin{aligned}(X^2-P)^2-Q+R&=(X^2-A^2)(X^2-B^2),\\ (X^2-P)^2-Q-R&=(X^2-C^2)(X^2-D^2),\end{aligned}$$

say, so that, corresponding to Dilcher's result,

$$\begin{aligned}A^2+B^2=2P&=C^2+D^2,\\ A^2B^2&=P^2-Q+R,\\ C^2D^2&=P^2-Q-R.\end{aligned}$$

It follows that

$$\begin{aligned}&A:B:C:D\\ &\quad=mp-nq:mq+np:mp+nq:mq-np,\end{aligned}$$

for integers m,n,p,q, and up to equivalence,

$$\begin{aligned}P&=(m^2+n^2)(p^2+q^2)/2,\\ Q&=((m^2-n^2)^2(p^2-q^2)^2+16m^2n^2p^2q^2)/4,\\ R&=2mnpq(m^2-n^2)(p^2-q^2).\end{aligned}$$

The second edition of [Crandall and Pomerance 05] gives a single example due to D. Symes of the extension to four nested squares:

$$\begin{aligned}&(((X^2-67405)^2-3525798096)^2\\ &\quad-5334707025515520 00)^2-469208209191321600^2\\ &=(X^2-11^2)(X^2-77^2)(X^2-101^2)(X^2-131^2)\\ &\quad\times(X^2-343^2)(X^2-353^2)(X^2-359^2)(X^2-367^2),\end{aligned}$$

allowing the product of sixteen integers to be accomplished with four squarings and four subtractions (this example is at variance with the assertion of [Dilcher 00, Section 3] that such an identity is impossible).

It is the purpose of the current note to investigate further this extension to four nested squares and to describe methods that produce two infinite families of such examples. Whether there can exist examples of such identities for five or more nested squares is an open question.

2. THE FIRST FAMILY

Suppose

$$\begin{aligned}&(((X^2-P)^2-Q)^2-R)^2-S^2\\ &\quad=(X^2-A^2)(X^2-B^2)(X^2-C^2)(X^2-D^2)(X^2-E^2)\\ &\qquad\times(X^2-F^2)(X^2-G^2)(X^2-H^2).\end{aligned}$$

Then

$$\begin{aligned}&(((X^2-P)^2-Q)^2-R-S)(((X^2-P)^2-Q)^2-R+S)\\ &\quad=(X^2-A^2)(X^2-B^2)(X^2-C^2)(X^2-D^2)(X^2-E^2)\\ &\qquad\times(X^2-F^2)(X^2-G^2)(X^2-H^2),\end{aligned}$$

so that we may take, say,

$$\begin{aligned}&((X^2-P)^2-Q)^2-R-S\\ &\quad=(X^2-A^2)(X^2-B^2)(X^2-C^2)(X^2-D^2),\\ &((X^2-P)^2-Q)^2-R+S\\ &\quad=(X^2-E^2)(X^2-F^2)(X^2-G^2)(X^2-H^2),\end{aligned}$$

equivalently,

$$\begin{aligned}&((X^2-P)^2-Q)^2-R-S\\ &\quad=(X^2-a)(X^2-b)(X^2-c)(X^2-d),\\ &((X^2-P)^2-Q)^2-R+S\\ &\quad=(X^2-e)(X^2-f)(X^2-g)(X^2-h),\end{aligned}$$

where

$$(a,b,c,d,e,f,g,h)=(A^2,B^2,C^2,D^2,E^2,F^2,G^2,H^2).$$

Equating powers of X^2 yields

$$\begin{aligned}&a+b+c+d\\ &\quad=4P=e+f+g+h,\\ &ab+ac+ad+bc+bd+cd\\ &\quad=6P^2-2Q\\ &\quad=ef+eg+eh+fg+fh+gh,\\ &abc+abd+acd+bcd\\ &\quad=4P^3-4PQ\\ &\quad=efg+efh+egh+fgh,\end{aligned}$$

and

$$\begin{aligned}abcd&=(P^2-Q)^2-R-S, \qquad (2\text{–}1)\\ efgh&=(P^2-Q)^2-R+S.\end{aligned}$$

	A	B	C	D	E	F	G	H
1*	−101	353	−77	359	343	131	367	11
	126	−227	141	−218	237	106	189	178
2*	−719	−827	139	1087	−541	953	317	−1049
	−773	54	613	−474	206	−747	−366	683
3*	−141	2428	1267	2076	916	2253	2324	717
	2287	−2569	3343	−809	3169	−1337	3041	1607
4	5093	9217	9677	4153	8473	6253	3167	10043
	7155	−2062	6915	2762	7363	1110	6605	−3438
5	5971	11287	5447	11549	3661	12233	9689	8317
	8629	−2658	8498	−3051	7947	−4286	9003	686
6	4825	17573	8677	16025	9935	15277	17923	3295
	11199	−6374	12351	−3674	12606	−2671	10609	7314
7	21523	4567	17593	13213	19483	10223	7493	20687
	13045	8478	15403	2190	14853	4630	14090	−6597
8	3031	32507	30109	12623	7397	31799	10129	31037
	17769	−14738	21366	8743	19598	−12201	20583	10454
9*	−171061	242103	−216799	202173	−194223	223949	−239961	174053
	35521	−206582	−7313	−209486	14863	−209086	−32954	−207007
10*	−50169	2324657	1368087	1880129	689137	2220729	2107393	982569
	1137244	−1187413	1624108	−256021	1454933	−765796	1544981	562412
11*	−42677861	19377903	−46331907	7089241	15833813	44115681	12179767	45260979
	−11649979	−31027882	−19621333	−26710574	29974747	−14140934	28720373	−16540606

TABLE 1. Computed solutions of the system (2–2).

Thus

$$\begin{aligned}
&a+b+c+d=e+f+g+h=4P,\\
&3(a^2+b^2+c^2+d^2)-2(ab+ac+ad+bc+bd+cd)\\
&\quad=3(e^2+f^2+g^2+h^2)\\
&\qquad-2(ef+eg+eh+fg+fh+gh)\\
&\quad=16Q,
\end{aligned}$$

and eliminating P, Q, we have

$$\begin{aligned}
a+b+c+d&=e+f+g+h,\\
ab+cd+(a+b)(c+d)&=ef+gh+(e+f)(g+h),
\end{aligned}$$

and

$$\begin{aligned}
(a+b-c-d)(a-b+c-d)(a-b-c+d)&=0,\\
(e+f-g-h)(e-f+g-h)(e-f-g+h)&=0,
\end{aligned}$$

with R, S deducible from equations (2–1). By the symmetry in a,b,c,d,e,f,g,h (for example, by interchanging b and c), we may suppose that

$$a+b=c+d,\quad e+f=g+h,$$

forcing

$$a+b=c+d=e+f=g+h,\quad ab+cd=ef+gh.$$

We are thus reduced to considering the variety V with equations

$$\begin{aligned}
A^2+B^2=C^2+D^2&=E^2+F^2=G^2+H^2,\\
A^2B^2+C^2D^2&=E^2F^2+G^2H^2,
\end{aligned}\tag{2–2}$$

which is a threefold of degree 32 in projective seven-dimensional space. Here, the corresponding P,Q,R,S take the form

$$\begin{aligned}
2P&=A^2+B^2,\\
2Q&=\left(\frac{A^2-B^2}{2}\right)^2+\left(\frac{C^2-D^2}{2}\right)^2,\\
2R&=\left(\frac{A^2B^2-C^2D^2}{2}\right)^2+\left(\frac{E^2F^2-G^2H^2}{2}\right)^2,\\
2S&=\left(\frac{A^2B^2-C^2D^2}{2}\right)^2-\left(\frac{E^2F^2-G^2H^2}{2}\right)^2.
\end{aligned}$$

It is worth remarking that the variety is also defined by the system

$$\begin{aligned}
A^2+B^2=C^2+D^2&=E^2+F^2=G^2+H^2,\\
A^4+B^4+C^4+D^4&=E^4+F^4+G^4+H^4,\\
A^6+B^6+C^6+D^6&=E^6+F^6+G^6+H^6,
\end{aligned}$$

and there is also the curious identity

$$(A^4-B^4)^2+(C^4-D^4)^2=(E^4-F^4)^2+(G^4-H^4)^2.$$

k	A E	B F	C G	D H
	... ...	... ...	... ...	... ...
-4	-5670199925485321 -17840344880113922	-25859765563651438 19560182431679401	-14276050600484041 -26446195555112642	22295134479397198 1215476393323561
-3	-190178281 6948421	376306787 421575967	-414329299 -217202597	78139673 -361382911
-2	613 -366	-474 683	773 -206	-54 747
1	-719 -541	-827 953	139 317	1087 -1049
2	-168094813 -289292754	-246234486 72090157	-93064253 -214262194	283242534 207313773
3	-8019083878913157 25230719161789081	36571185079881239 27661671948436203	-31529965489136759 1719837551565479	20189565638166117 -37400527311793323
	... ...	... ...	... ...	... ...

TABLE 2. Solutions to (2–2) in the first family.

Solutions arise naturally in pairs: if

$$(A, B, C, D, E, F, G, H)$$

provides a solution, then so does

$$(A+B, A-B, C+D, C-D, E+F, E-F, G+H, G-H).$$

Table 1, of particular solutions (listed in pairings), was computed directly by Michael E. Paul.

The starred solutions satisfy the equation

$$A - C = E - G; \tag{2–3}$$

further, the second starred solution satisfies

$$A + B + C + D = E + F + G + H. \tag{2–4}$$

It turns out that the intersection of the variety V with the two hyperplanes given by (2–3) and (2–4) is a reducible curve, one of whose components is an elliptic curve with positive rational rank. Thus we can construct infinitely many rational points on V.

In the first instance, we investigate solutions of the system (2–2) subject to the restriction at (2–3). Put

$$A = -s + t, \quad C = s + t, \quad E = -s + u, \quad G = s + u;$$

then solving the system of equations (2–2) yields

$$(B^2, D^2, F^2, H^2) = (5s^2 + 2st + u^2,\ 5s^2 - 2st + u^2,\ 5s^2 + 2su + t^2,\ 5s^2 - 2su + t^2).$$

The first equation represents a quadric surface with parameterization

$$B : s : t : u = 2\lambda\mu : 2\lambda^2 : \mu^2 - \nu^2 - 5\lambda^2 : 2\lambda\nu,$$

and similarly, from the second equation,

$$D : s : t : u = 2\theta\phi : 2\theta^2 : -(\phi^2 - \psi^2 - 5\theta^2) : 2\theta\psi.$$

For compatibility we require

$$\lambda : \nu = \theta : \psi, \quad \mu^2 - \nu^2 - 5\lambda^2 : 2\lambda\nu = -\phi^2 + \psi^2 + 5\theta^2 : 2\theta\psi,$$

and without loss of generality we may take $\psi = \nu$, $\theta = \lambda$, so that

$$\mu^2 + \phi^2 = 2\nu^2 + 10\lambda^2,$$

a quadric surface with parameterization

$$\mu : \phi : \nu : \lambda = 10z^2 + x^2 + 2xy - y^2 : 10z^2 - x^2 + 2xy + y^2 : 10z^2 - x^2 - y^2 : 2z(x + y).$$

This in turn leads to

$$s : t : u = 2(x + y)z^2 : (x - y)(xy + 5z^2) : z(-x^2 - y^2 + 10z^2),$$

and we set

$$\begin{aligned} A &= x^2y - xy^2 + 3xz^2 - 7yz^2, \\ C &= x^2y - xy^2 + 7xz^2 - 3yz^2, \\ E &= -z(x^2 + y^2 + 2xz + 2yz - 10z^2), \\ G &= -z(x^2 + y^2 - 2xz - 2yz - 10z^2), \end{aligned}$$

with

$$B = z(x^2 + 2xy - y^2 + 10z^2),$$
$$D = -z(x^2 - 2xy - y^2 - 10z^2).$$

It remains to satisfy

$$\begin{aligned} F^2 = {} & x^4y^2 - 2x^3y^3 + x^2y^4 \\ & + 10x^3yz^2 - 20x^2y^2z^2 + 10xy^3z^2 \\ & - 4x^3z^3 - 4x^2yz^3 - 4xy^2z^3 - 4y^3z^3 + 45x^2z^4 \\ & - 10xyz^4 + 45y^2z^4 + 40xz^5 + 40yz^5 \end{aligned} \tag{2–5}$$

and

$$\begin{aligned} H^2 = {} & x^4y^2 - 2x^3y^3 + x^2y^4 \\ & + 10x^3yz^2 - 20x^2y^2z^2 + 10xy^3z^2 + 4x^3z^3 \\ & + 4x^2yz^3 + 4xy^2z^3 + 4y^3z^3 + 45x^2z^4 \\ & - 10xyz^4 + 45y^2z^4 - 40xz^5 - 40yz^5. \end{aligned} \tag{2–6}$$

If we now also assume the restriction (2–4), then we have the following equation in addition to equations (2–5) and (2–6):

$$F+H = 2x^2y-2xy^2+2x^2z+4xyz+2y^2z+10xz^2-10yz^2.$$

Eliminating F, H results in

$$\begin{aligned} & (x+y)(x-z)z(y+z) \\ & \quad \times (x^2y - xy^2 + x^2z + y^2z + 5xz^2 - 5yz^2 - 10z^3) \\ & \quad \times (2x^3y - 4x^2y^2 + 2xy^3 + x^3z + 13x^2yz - 13xy^2z \\ & \qquad - y^3z + 16x^2z^2 + 16y^2z^2 + 60xz^3 - 60yz^3 \\ & \qquad + 40z^4) = 0. \end{aligned}$$

The linear factors correspond to degenerate solutions, and the curve corresponding to

$$x^2y - xy^2 + x^2z + y^2z + 5xz^2 - 5yz^2 - 10z^3 = 0$$

is birationally equivalent to the elliptic curve

$$Y^2 = X^3 - 2X + 1,$$

with rational rank 0.

However the curve corresponding to

$$\begin{aligned} & 2x^3y - 4x^2y^2 + 2xy^3 + x^3z + 13x^2yz - 13xy^2z \\ & \quad - y^3z + 16x^2z^2 + 16y^2z^2 + 60xz^3 - 60yz^3 \\ & \quad + 40z^4 = 0 \end{aligned}$$

is birationally equivalent to the elliptic curve

$$Y^2 = (X-4)(X-3)(X+6), \tag{2–7}$$

with rational rank 1. The birational map is given by

$$\begin{aligned} (X,Y) = {} & \big((2x^2 - 2xy + 7xz + yz - 2z^2)/(2z^2), \\ & (2x^3 - 4x^2y + 2xy^2 + 10x^2z - 9xyz \\ & \quad - y^2z - 2xz^2 + 14yz^2 - 30z^3)/(2z^3)\big), \end{aligned}$$

with inverse

$$\begin{aligned} & (x,y,z) \\ & \quad = \big((-21+4X)(3-10X+2X^2+Y), \\ & \qquad 171 + 102X - 44X^2 - 69Y - 4XY, \\ & \qquad (-21+4X)(-15+5X+2Y)\big). \end{aligned}$$

A generator of infinite order on (2–7) is given by $P = (2,4)$. Corresponding to the multiples kP of P, (A,B,C,D,E,F,G,H) are given in Table 2.

3. THE SECOND FAMILY

If we suppose next that only the restriction (2–3) holds, then by investigation of the numerical data within Table 1, we discover that the following curve $\mathcal{C}$ of genus 1 plays a crucial role:

$$\mathcal{C} : 3x^2y-4xy^2+y^3+(x^2-14xy+9y^2)z+10(x+y)z^2 = 0.$$

For if (x,y,z) is a point on $\mathcal{C}$, then we obtain from (2–5), (2–6), that

$$\begin{aligned} F = {} & -2x^2y + 3xy^2 - y^3 - (x^2 - 8xy + 7y^2)z \\ & - (x+3y)z^2, \\ H = {} & -x^2y + xy^2 + (6xy - 2y^2)z + (3x - 11y)z^2. \end{aligned}$$

In summary, a point (x,y,z) of $\mathcal{C}$ leads to the solution of the system (2–2) given by

$$\begin{aligned} A &= x^2y - xy^2 + (3x-7y)z^2, \\ B &= z(x^2 + 2xy - y^2 + 10z^2), \\ C &= x^2y - xy^2 + (7x-3y)z^2, \\ D &= -z(x^2 - 2xy - y^2 - 10z^2), \\ E &= -z(x^2 + y^2 + 2(x+y)z - 10z^2), \\ F &= -2x^2y + 3xy^2 - y^3 - (x^2 - 8xy + 7y^2)z \\ &\quad - (x+3y)z^2, \\ G &= -z(x^2 + y^2 - 2(x+y)z - 10z^2), \\ H &= -x^2y + xy^2 + (6xy - 2y^2)z + (3x - 11y)z^2. \end{aligned}$$

All such solutions satisfy the linear condition $A - C = E - G$.

k	x	y	z	A E	B F	C G	D H
0	1	1	0				
1	1	3	0				
2	0	0	1				
3	1	0	0				
4	2	−4	1				
5	25	55	3	−367 −101	11 −353	−343 −77	131 359
6	23	21	4	−141 −2324	2428 −717	1267 −916	2076 2253
7	−177	−201	11	239961 −171061	174053 −242103	194223 −216799	223949 202173
8	−115	−185	84	117035 88212	110532 −39909	−3925 −32748	160932 220117
9	−305	157	737	−12179767 46331907	45260979 −7089241	−15833813 42677861	44115681 −19377903
10	10652	−604	777	−1204133636 −2283033607	1965994297 320669516	−626393732 −1705293703	−2218716359 1551465364
...	...	...	...	... ...	... ...	... ...	... ...

TABLE 3. Solutions to (2–2) in the second family.

Choosing the point $(x, y, z) = (1, 1, 0)$ as base point on $\mathcal{C}$ shows that the curve is birationally equivalent to the curve $\mathcal{E}$ given by

$$\mathcal{E} : Y^2 = X^3 - X^2 - 8X + 112,$$

an elliptic curve of rank 1 over $\mathbb{Q}$ with no rational torsion and generator $P = (12, 40)$ corresponding to $Q(x, y, z) = (1, 3, 0)$ on $\mathcal{C}$.

The multiples kQ of Q on $\mathcal{C}$ shown in Table 3 deliver nondegenerate solutions to the system given by (2–2) (we observe that the multiple $-kQ$ returns a symmetry of the solution at kQ).

ACKNOWLEDGMENTS

I am extremely grateful to Michael E. Paul for computing solutions given in Table 1 and for several fruitful e-mail discussions.

REFERENCES

[Crandall 96] R. E. Crandall. *Topics in Advanced Scientific Computation*, TELOS (The Electronic Library of Science). New York: Springer-Verlag, 1996.

[Crandall and Pomerance 01] R. E. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective* New York: Springer-Verlag, 2001.

[Crandall and Pomerance 05] R. E. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective*, 2nd ed. New York: Springer-Verlag, 2005.

[Crandall et al. 97] R. E. Crandall, K. Dilcher, and C. Pomerance. "A Search for Wieferich and Wilson Primes." *Math. Comp.* 66:217 (1997), 433–440.

[Dilcher 00] K. Dilcher. "Nested Squares and Evaluations of Integer Products." *Experimental Mathematics* 9:3 (2000), 369–372.

Andrew Bremner, Department of Mathematics and Statistics, Arizona State University, Tempe AZ 85287-1804
(bremner@asu.edu)

Received October 30, 2007; accepted January 27, 2008.