My Favorite Elliptic Curve: A Tale of Two Types of Triangles

Richard K. Guy

One of the many beauties of elliptic curves is their blend of arithmetic and geometry, not only intrinsically but also in their applications. If you want to learn more about them there are several good introductions available: Silverman & Tate [**9**], Knapp [**7**] and Cassels [**2**], who manages to write a whole book on elliptic curves without using the word 'rank.'

The curve of the title (88A in [**1**] or [**4**]) is:

$$Y^2 = X^3 - 4X + 4$$

Figure 1 shows a picture of part of its part. It's fairly uncomplicated curve: it has only one real component and doesn't break up into an 'egg' and an infinite branch as many elliptic curves do. Moreover, it doesn't have any **torsion points**, points of finite order, except for the point at infinity, which we must always remember. And I thank the referee for reminding me that when I say 'torsion points' this is an ellipsis for '**rational** torsion points.' For example, the points of inflexion are of order three, but they are not rational on this curve. One of the difficulties for the beginner is keeping track of what field he is working in: it is often convenient to vary the focus from complex to real to rational, and even to consider finite fields.

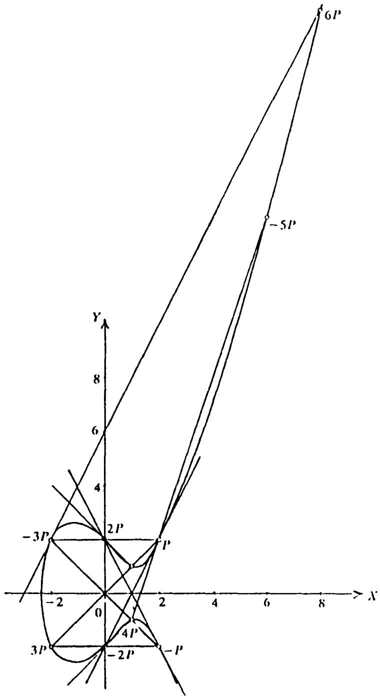

Figure 1. The elliptic curve $Y^2 = X^3 - 4X + 4$.

The curve does have several obvious rational points.

$$(0, \pm 2), \qquad (1, \pm 1), \qquad (2, \pm 2), \qquad (-2, \pm 2).$$

The points of an elliptic curve form a group. Take the point at infinity as the (additive) identity, 0. The group law is described by noting that a straight line meets a cubic curve in three points whose sum we define to be 0. For example, the ordinate $X = 2$ meets the curve in $(2, \pm 2)$ and the point at infinity, so if $(2, \pm 2)$ are P and Q, then

$$P + Q + 0 = 0$$

and $Q = -P$. The tangent at $(2,2)$ meets the curve again at $(0, -2) = R$, say, so that

$$P + P + R = 0,$$

$R = -2P$ and $(0,2) = 2P$. On joining this to P we see that $(-2,2) = -3P$, $(-2, -2) = 3P$. By joining $-P$ to $-3P$ or drawing the tangent at $-2P$ we discover that $4P = (1, -1)$ and then $5P = (6, -14), 6P = (8,22)$ and so on. We soon convince ourselves that there is an infinity of rational points on the curve. In fact a theorem of Mazur (see **[6]**, p. 223, Theorem 7.5, for example) tells us that there can't be more than 16 rational points of finite order. The **rank** of the curve is 1; all rational points can be derived from the **generator** $P = (2,2)$.

Warning: to *prove* that a point is a generator usually requires more sophistication than we display here.

A mixture of cevians. Problem E3434 in the April 1991 MONTHLY asked, or should have asked, for integer triangle ABC in which the median from A, the bisector of angle B, and the altitude from C are concurrent. At the time of writing, no solution has been published, though I have seen an interesting one due to J. G. Mauldon, which makes no explicit use of an elliptic curve.

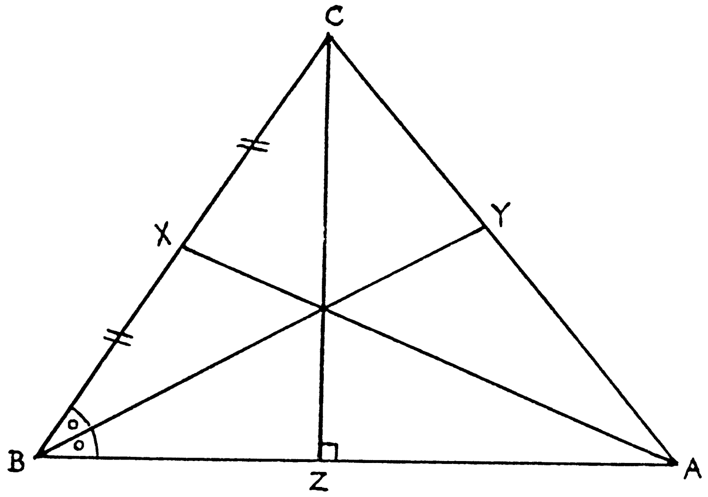

Figure 2. Triangle with concurrent median, angle-bisector and altitude.

Ceva's theorem ([3, p.4] for example) tells us that three concurrent lines drawn from the vertices of a triangle divide the sides in ratios whose product is 1:

$$\frac{BX}{XC}\cdot\frac{CY}{YA}\cdot\frac{AZ}{ZB}=1, \qquad \frac{a/2}{a/2}\cdot\frac{a}{c}\cdot\frac{b\cos A}{a\cos B}=1$$

where the middle ratio comes from the angle-bisector theorem. Multiply $b\cos A = c\cos B$ by $2ac$ and the cosine formula gives

$$a(b^2+c^2-a^2)=c(c^2+a^2-b^2).$$

Put

$$Y=\frac{2b}{a+c}, \qquad X=\frac{2c}{a+c}$$

and we get our favorite curve

$$Y^2=X^3-4X+4.$$

So we seem to have found an infinity of such triangles, but a complication is that not all rational points on the curve give real triangles. The transformation we just made inverts to

$$(a:b:c)=(2-X:Y:X).$$

We can change the signs of all three of a, b and c, so we do this if necessary to make a positive. We can change the sign of Y, since the curve is symmetrical, and so make b positive. And we can interpret either sign for c: when c is negative, Y divides CA externally in the ratio $a:c$ and BY is the *external* bisector of angle B (Figure 3).

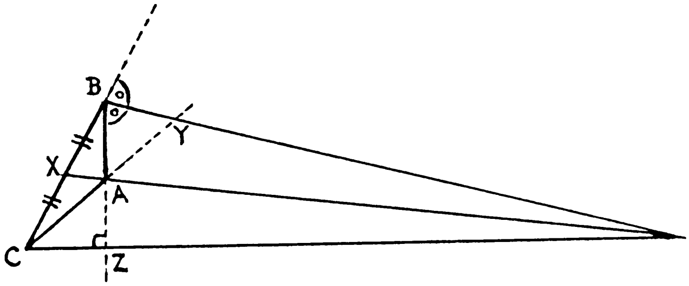

Figure 3. Triangle with external angle-bisector concurring with median and altitude.

If $X>0$ the triangle inequality requires that $Y>2X-2$, $Y>2-2X$ and $2>Y$, i.e. that we are inside the region in Figure 1 bounded by the tangents at $\pm P$ and the line $Y=2$, i.e. on the piece of curve $0<X<2, 0<Y<2$. Such points give us genuine internal bisector triangles. The point $-4P$ corresponds to the equilateral triangle.

If $X<0$ the triangle inequality gives $Y>-2$, $Y>2$ and $2-2X>Y$. We are on the piece of the curve below the tangent at $-P$ and above the line $Y=2$: i.e. $-2<X<0, Y>2$. These points give triangles whose external angle-bisector concurs with the median and altitude.

If X is outside the interval $[-2,2]$, the triangle inequality is not satisfied. Table 1 lists a point, chosen so that $(2-X)Y$ is positive, from each of the first twenty pairs; together with the associated triple (a,b,c) and a description of the resulting

TABLE 1. Points on curve and corresponding triangles.

point	(X,Y)	(a,b,c)	
P	$(2,2)$	$(0,1,1)$	D
$2P$	$(0,2)$	$(1,1,0)$	D
$-3P$	$(-2,2)$	$(2,1,-1)$	D
$-4P$	$(1,1)$	$(1,1,1)$	G(Δ)
$5P$	$(6,-14)$	$(2,7,-3)$	N
$-6P$	$(8,-22)$	$(3,11,-4)$	N
$7P$	$(10/9,26/27)$	$(12,13,15)$	G
$8P$	$(-7/4,19/8)$	$(30,19,-14)$	A
$-9P$	$(-6/25,278/125)$	$(140,139,-15)$	A
$-10P$	$(88/49,554/343)$	$(35,277,308)$	G
$11P$	$(310,-5458)$	$(308,5458,-310)$	N
$-12P$	$(273/11^2,-3383/11^3)$	$(341,3383,-3003)$	N
$13P$	$(206/31^2,52894/31^3)$	$(26598,26447,3193)$	G
$-14P$	$(-3344/39^2,87326/39^3)$	$(124527,43663,-65208)$	N
$-15P$	$(9362/103^2,1175566/103^3)$	$(610584,587783,4832143)$	G
$16P$	$(27105/76^2,-4131247/76^3)$	$(1182028,4131217,-2059980)$	N
$-17P$	$(256882/151^2,-128313838/151^3)$	$(31903280,128313838,-38789182)$	N
$18P$	$(589456/695^2,324783646/695^3)$	$(130866415,162391823,204835960)$	G
$19P$	$(-2280402/1247^2,5023772066/1247^3)$	$(3360926870,2511886033,-1421830647)$	A
$-20P$	$(-1896655/1939^2,17691806567/1939^3)$	$(18257812083,17691806567,-3677614045)$	A

triangle, if any: D means degenerate, G is good, N does not yield a real triangle, while A means that the angle-bisector is external.

The point $11P$ is a pleasant surprise, though it would be natural to join $5P$ to $6P$ if one were looking for large integer points. Note that there can only be a finite number of integer points, i.e., points with integer coordinates. This is Siegel's theorem [see **8**, p. 247, Theorem 3.1, for example]. Fortunately for us, any rational point will do, because the determination of all integer points requires some ingenuity, Tzanakis & Weger [**13**, **14**] have made some progress with this problem; Zagier's paper [**15**] explains the connexion with the magic number g that we'll meet below. Indeed, since this paper was first drafted, a method using these **elliptic logarithms** has been developed by Stroeker & Tzanakis [**11**] (and independently by Gebel, Pethö & Zimmer [**5**]) and used by Stroeker & de Weger [**12**] to settle the problem of the Ochoa curve [**6**].

As $11P$ is quite near infinity, 11 serves as an almost period, with $12P$ near P, $13P$ near $2P$, etc. so that one can predict that (for some distance), $4P, 7P, 10P, 13P, 15P, 18P, 21P, 24P, 26P, 29P, 32P, \ldots$ will give good triangles, and that $8P, 9P, 19P, 20P, 30P, 31P, \ldots$ will give external bisector ones, although eventually there will be a hiccup, when a better approximation to the period takes over. About $4/11$ of the points give genuine triangles, and about $2/11$ give triangles in which it is the external bisector which concurs with the median and altitude. If you want better approximations to these fractions, or want to know just when the hiccup occurs, read on.

The 'near periods' are associated with 'large' points, such as

$$72P = (4543.72\ldots, 306279.98\ldots)$$

$$227P = (6619.74\ldots, -538594.19\ldots)$$

$$299P = (154460.66\ldots, 60705331.35\ldots)$$

$$1722P = (5373628.48\ldots, 12456655569.68\ldots)$$

These are found from the convergents to the continued fraction of the number g, defined as

$$\frac{1}{2\Omega}\int_2^\infty \frac{dX}{Y} = 0.81939599219381946697456537 71\ldots$$

$$= [0,1,4,1,1,6,3,1,4,1,4,1,8,1,4,1,8,7,5,14,14,1,1,1,1,1,2,\ldots]$$

where 2Ω is the **real period** of the curve (see later for more detail) and the lower terminal of the integral is the X-coordinate of the generator. The convergents are

$$\frac{0}{1}, \frac{1}{1}, \frac{4}{5}, \frac{5}{6}, \frac{9}{11}, \frac{59}{72}\, \frac{186}{227}, \frac{245}{299}, \frac{1166}{1423}, \frac{1411}{1722}, \frac{6810}{8311}, \frac{8221}{10033}, \frac{39694}{48443}, \frac{47915}{58476}, \ldots$$

whose denominators $5, 6, 11, 72, 227, 299\ldots$ are good candidates for a 'near period.' The lines joining $-P$ to $11P$, $-72P, 227P$, $-299P, \ldots$ are closer and closer to the vertical, so that the points $-10P, 73P$, $-226P, 300P, \ldots$ are nearer and nearer to $P = (2,2)$; the signs have been chosen alternately so that the X-coordinates, $1.7959\ldots, 1.9423\ldots, 1.9520\ldots, 1.9898\ldots$ are less than 2: remember that the convergents are alternately less or greater than g. Figure 4 shows part of the curve magnified to illustrate the near periodicity: note that points closest together differ by $72P$.

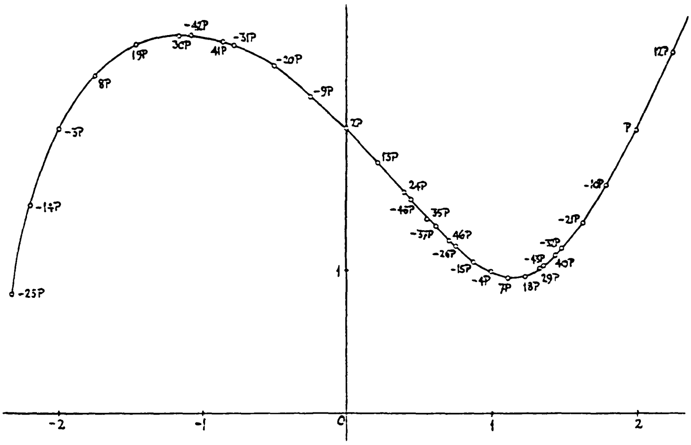

Figure 4. Curve magnified to show 11 and 72 as near periods.

An elliptic curve over the complex field should be thought of as a torus, with the real part as a circle, compactified by the point at infinity. There's a second circle if the curve has an 'egg." Figure 5 is a diagrammatic representation of the first 25 pairs of points $\pm kP$ whose labels are outside the circle and the fractional part of $kg, kg - \lfloor kg \rfloor$, is written inside the circle. The X-coordinate increases across the horizontal diameter on some curious scale, presumably related to the Weierstaß $\wp$-function. The regions of Figure 5 are labelled with the letters from the last column of Table 1. The ordinates $x = -2$, 0 and 2 give degenerate triangles, D, and the ordinate $x = 1$ corresponds to the equilateral triangle, $\triangle$.

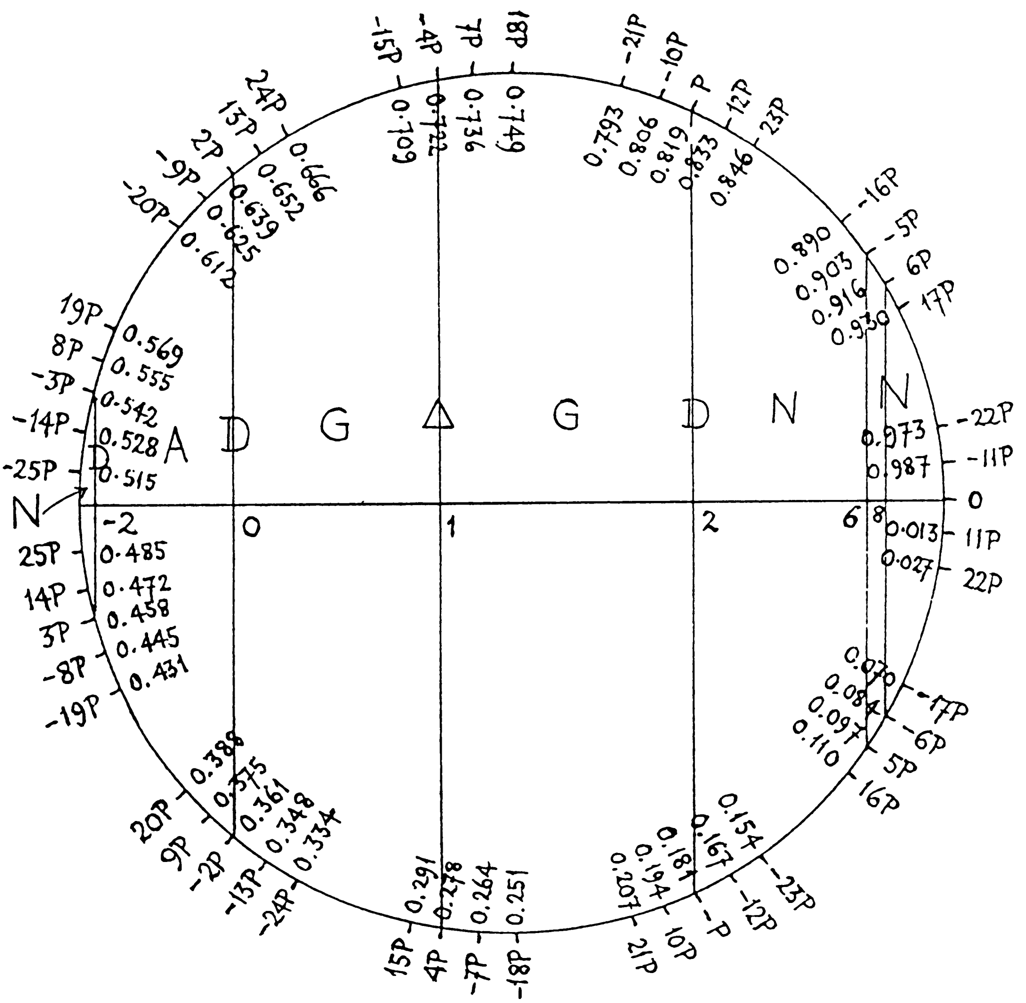

Figure 5. Diagrammatic representation showing near periodicity.

Of course, we've now given away our secret. You will have noticed that as your calculate successive points, the numbers of digits in their coordinates increase in size rather alarmingly. But the magic number g will tell us just where any point kP is: calculate the fractional part of kg and look at Figure 5. For example, $73P$ gives a good triangle (whose sides have about 140 decimal digits!) but $84P$ does not; $70P$ is good, but $81P$ requires the external bisector interpretation, as do $74P$ and $75P$.

Let E denote the set of **real** solutions (a, b) to the equation $Y^2 = X^3 - 4X + 4$ together with the point at infinity. The real period is defined by the integral.

$$2\Omega = \int_{\alpha}^{\infty} \frac{dX}{Y} = \int_{\alpha}^{\infty} \frac{dX}{\sqrt{X^3 - 4X + 4}}$$

where α is the real root of $X^3 - 4X + 4$. Then it is true (but not so easy to prove) that there is a group isomorphism

$$\phi : E \to \frac{\mathbb{R}}{2\Omega\mathbb{Z}} \qquad (a, b) \mapsto \int_{a}^{\infty} \frac{dX}{Y}$$

Thus the magic number g is really $g = \phi(P)$, and this explains exactly why kg being near to $2\Omega\mathbb{Z}$ is equivalent to kP being close to the point at infinity.

Here are the fractional parts of kg for the best candidates:

k	72	227	299	1423	1722	8311
	0.9965	0.0029	0.999402	0.000497	0.999899	0.000091

Problem for experts. Good approximations to a continued fraction come from truncating it just before a large partial quotient. Our continued fraction doesn't display any spectacular partial quotients, but those for several curves do. For example, curve 37A, $y(y+1) = x(x^2-1)$, has, for the magic number associated with its generator, $(0,0)$:

$$[0;3,4,1,1,5,2,\mathbf{168},\mathbf{46793},1,7,1,51,1,7,1,6,2,1,1,1,10,1,2,10,1,2,11,$$
$$16,3,1,1,1,1,4,1,1,3,1,1,5,5,25,1,34,10,2,18,10,\mathbf{585},1,2,3,1,1,\mathbf{440},1,$$
$$1,7,2,1,4,6,16,5,2,3,2,5,1,1,77,1,2,1,1,1,13,51,3,1,2,1,4,4,3,1,10,5,$$
$$1,1,1,2,1,32,8,1,2,1,4,61,\dots]$$

What is going on? Something akin to what is described by Stark in [**10**]?

Isosceles Heron triangles. Colleague Bill Sands is always looking for problems for *Crux Mathematicorum*; he asked if there were triangles with integer sides and area associated with rectangles having the same perimeter and area. There are indeed many such, but none of them right-angled, which is what he originally asked for. This last statement can be confirmed via curve 14A4, which has rank 0 and whose six torsion points yield only degenerate triangles. A discussion of the general problem may appear elsewhere; and see the last section for an introduction.

But here we find an infinite family of **isosceles** triangles. Let the equal legs be $m^2 + n^2$ and the base be $2(m^2 - n^2)$ so that the altitude in $2mn$:

$$\text{the semiperimeter} = p + q = 2m^2$$

$$\text{and the area} = pq = 2mn(m^2 - n^2)$$

where p and q are the sides of the associated rectangle. So we require that

$$(p-q)^2 = 4m^4 - 8mn(m^2 - n^2)$$

shall be a perfect square. If we write

$$X = \frac{2n}{m}, \qquad Y = \frac{p-q}{m^2}$$

what do we get?

$$Y^2 = X^3 - 4X + 4.$$

This time all rational points give rational triangles which are realized geometrically, provided that when n is outside the interval $[0, m]$ we are willing to consider negative lengths and areas. In calculating the perimeters, sometimes the base of the triangle or one of the sides p, q of the rectangle must be taken as negative.

For comparison with the first family of triangles we use the same multiples of P as before, though now a change in sign of Y merely interchanges the roles of p and q. Write $X = x/d^2, Y = y/d^3$ where x, y, d are integers with $d > 0, x \perp d$, $y \perp d$ (that is, x and y are each prime to d). Note that x and y are not necessarily prime to one another: in fact x_k and y_k are both even unless k is a multiple of 4, when they are both odd, while d_k is odd unless k is a multiple of 8.

We have seen that (X_{k+1}, Y_{k+1}) may be found by joining (X_k, Y_k) to $P = (X_1, Y_1) = (2, 2)$:

$$X_{k+1} = \frac{2(X_k^2 - 2Y_k)}{(X_k - 2)^2} = \frac{2n_k}{m_k} \qquad Y_{k+1} = \frac{4(X_kY_k - 3X_k^2 + 6X_k - 4)}{(X_k - 2)^3}$$

$$\frac{x_{k+1}}{d_{k+1}^2} = \frac{(x_k^2 - 2y_kd_k)}{(x_k - 2d_k^2)^2} \qquad \frac{m_{k+1}}{n_{k+1}} = \frac{(x_k - 2d_k)^2}{x_k^2 - 2y_kd_k}$$

We choose $m \perp n$ and $m > 0$; the g.c.d., (m_{k+1}, n_{k+1}), of the numerator and denominator of the last fraction is $2d_{k-1}^2$, $16d_{k-1}^2$, $4d_{k-1}^2$ or $4d_{k-1}^2$ according as $k \equiv 0$, 1, 2, or $3 \bmod 4$.

Table 2 lists information about the first 20 isosceles triangles and is parallel to Table 1. We do not list (m, n) since these are $(2d^2, x)$ or $(d^2, x/2)$ according as 4 divides k or not. If m and n are both odd, as they are when k is odd, we keep the triangle primitive by dividing all lengths by 2. The rectangle sides p and q are $2d(2d^3 \pm y)$ or have $\frac{1}{4}$ or $\frac{1}{8}$ of those values according as $4|k$, $2\|k$ is odd. As they are each divisible by d, primitive rectangles can only be given by integer points, so that $k = 5$ and $k = 11$ are the only nontrivial examples.

The labels are the same as before, except that the interpretation of A is now: altitude and area are negative and the rectangle $p \times q$ has $q < 0 < p$, while N now means that the base of the triangle is negative, the altitude is positive or negative according as $n > m$ or $n < -m$, the area and p each have sign opposite to that of the altitude, and $q > 0$. The latter case is exemplified by $14P$ where the area is positive, but in calculating the perimeter of the triangle, its base must be taken as negative.

Shapes of triangle. In each problem, as the point moves on the curve, the shape of the triangle changes continuously. As the rational points are dense on the curve, we can approximate to any shape of triangle that is consistent with the geometrical properties that have been imposed.

The cevians triangle, for example, can be as near right-angled at C as we wish. Choose a point with X-coordinate as near to $\sqrt{5} - 1 = 1.236\ldots$ as required. The point $18P$ gives a triangle with $A = 39.68°, B = 52.40°, C = 87.92°$. The other angles approach 90° simultaneously, though not quite at the same speed, as the triangle degenerates when we approach $X = 0$; the $70P$ triangle has $A = 89.95°, B = 88.32°, C = 1.73°$. In this problem the triangle can be equilateral, corresponding to the point $4P$, and points close by to the left or right give triangles with one or two angles less than 60°: $68P$: $A, B, C) = (62{,}40°, 60.98°, 56.60°)$ $76P$: $(A, B, C) = (57.51°, 59.02°, 63.47°)$.

The Heron triangles are isosceles, so don't display such variety. They vary from degeneracy one way to the other: this incarnation of $70P$ gives base angles of 3.35°, while $73P$ corresponds to base angles of 88.325°. The vertical angle can also be as near to 90° as we wish: the points $15P$, $31P$, $41P$ and $57P$ give 84.7°, 93.8°, 86.3* and 87.9°.

The Heron triangles cannot be equilateral, but we can approximate by taking points near to the maxima and minima of the curve, $X = \pm 2/\sqrt{3} = \pm 1.1547\ldots$. Already $4P$: $(5, 5, 6)$ and $7P$: $(53, 53, 56)$ are quite good. Next better is $30P$ with base angles 60.525°.

TABLE 2. Isosceles triangles $(m^2 + n^2, m^2 + n^2, 2(m^2 - n^2))$ and rectangles $p \times q$ with common perimeter and area.

k	x	y	d	altitude	equal legs	base
1	2	2	1	1	1	0
2	0	2	1	0	1	2
−3	−2	2	1	−1	1	0
−4	1	1	1	4	5	6
5	6	−14	1	3	5	−8
−6	8	−22	1	8	17	−30
7	10	26	3	45	53	56
8	−7	19	2	−112	113	30
−9	6	278	5	−75	317	616
−10	88	554	7	4312	4337	930
11	310	−5458	1	155	12013	−24024
−12	273	−3383	11	132132	133093	−31930
13	206	52894	31	98983	467065	912912
−14	−3344	87326	39	−5086224	5109025	−964286
−15	9362	1175566	103	49660729	67231321	90639120
16	27105	−4131247	76	626233920	868129729	−1202464642
−17	256882	−128313838	151	2928583241	8508488041	−15977204880
18	589456	324783646	695	284721984400	320177744609	292897113232
19	−2280402	5023772066	1247	−1773022816809	1859055655241	1117994669680
−20	−1896655	17691806567	1939	−28523574533020	60139308180389	105889415604678

k	area	rectangle (p, q)	
1	0	(1, 0)	D
2	0	(2, 0)	D
−3	0	(1, 0)	D
−4	12	(6, 2)	G
5	−12	(−3, 4)	N
−6	−120	(−10, 12)	N
7	1260	(60, 21)	G
8	−1680	(140, −12)	A
−9	−23100	(660, − 35)	A
−10	2005080	(462, 4340)	G
11	−1861860	(−1364, 1365)	N
−12	−2109487380	(−15862, 13299)	N
13	45181384348	(871689, 51832)	G
−14	2452287298032	(4016298, 610584)	N
−15	2250602387559240	(86546265, 26004616)	G
16	−376512073310528320	(−494500840, 761398248)	N
−17	−23395287224795708040	(−4583904584, 5103790185)	N
18	41697123659341318400400	(346175467610, 120450833640)	G
19	−991115029206740553325560	(2775187436616, −357134446535)	A
−20	−1510172319128981992388733780	(125150833858190, −12066817875462)	A

A third manifestation. With help from Andrew Bremner we are investigating the general problem of finding triangle-rectangle pairs with common perimeter and common area.

Brahmagupta taught us that all Heron triangles are of shape

$$c(a^2 + b^2), \qquad b(a^2 + c^2), \qquad (b + c)(a^2 - bc),$$

which, if we take the third side as base, has altitude $2abc$, are $\Delta = abc(a + b)(a^2 - bc)$ and semiperimeter $s = a^2(b + c)$.

If the associated rectangle is $p \times q$, then we have $\Delta = pq$, $s = p + q$, and

$$(p - q)^2 = a^4(b + c)^2 - 4abc(b + c)(a^2 - bc)$$

must be a perfect square. Set $\mathscr{Y} = (p - q)/a^2(b + c), \mathscr{X} = bc/a^2$, $\mathscr{Z} = a/(b + c)$ and the equation becomes

$$\mathscr{Y}^2 = 1 - 4\mathscr{X}\mathscr{Z} + 4\mathscr{X}^2\mathscr{Z}.$$

However, in order that this transformation be birational, we also require that

$$1 - 4\mathscr{X}\mathscr{Z}^2 = \left(\frac{b - c}{b + c}\right)^2 = \mathscr{W}^2$$

be a perfect square. On eliminating $\mathscr{Z}$,

$$(\mathscr{Y}^2 - 1)^2 = 16\mathscr{Z}^2\mathscr{X}^2(\mathscr{X} - 1)^2 = 4\mathscr{X}(\mathscr{X} - 1)^2(1 - \mathscr{W}^2)$$

we have a quintic surface [which deserves study in its own right]. It contains a dozen straight lines, two of which, $\mathscr{X} = 1, \mathscr{Y} = \pm 1$, are double, so that a plane through either of them, say

$$n(\mathscr{Y} - 1) = m(\mathscr{X} - 1)$$

cuts the surface in a cubic curve.

So we can find "all" triangle-rectangle pairs in the following sense. Such a pair corresponds to a rational point on the quintic surface. This determines (m, n), the 'slope' of the plane through the point and the line $\mathscr{X} = 1, \mathscr{Y} = 1$. Elimination of $\mathscr{Y}$ between the surface and the plane, yields, on writing $x = -m^4\mathscr{X}, y = 2m^4n^2\mathscr{X}\mathscr{W}$:

$$y^2 = x\left[x^2 + 2(m^4 - 2m^3n + 2n^4)x + m^6(m - 2n)^2\right],$$

an elliptic curve whose rational points give all triangle-rectangle pairs of 'slope' (m,n). We are studying the range $0 < |m| \leq \mathrm{n} \leq 50$.

The discriminant of the curve is $4m^{12}n^4(m - 2n)^4(m^4 - 2m^3n + n^4)$ and the curve is singular just if $m = 0$, $n = 0$, $m = n$ or $m = 2n$. The torsion group is $\mathbb{Z}/4\mathbb{Z}$, the points $(-m^3(m - 2n), \pm 2m^3n^2(m - 2n))$ being of order 4. However, if $m^4 - 2m^3n + n^4 = r^2$ is a perfect square, then the torsion group is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, there being additional points $(m^3(m - 2n), \pm 2m^4(m - n)(m - 2n))$ of order 4 and $((r - n^2)^2, 0)$ and $((r + n^2)^2, 0)$ of order 2.

When is $m^4 - 2m^3n + n^4$ a perfect square? Put

$$\frac{r}{m^2} = \frac{X}{2} - \frac{n^2}{m^2} \quad \text{and} \quad \frac{n}{m} = \frac{Y + 2}{2X}$$

and what do you get?

$$\boxed{\mathrm{Y}^2 = \mathrm{X}^3 - 4\mathrm{X} + 4}$$

REFERENCES

1. B. J. Birch & W. Kuyk (editors), *Modular Functions of One Variable* IV (*Proc. Internat. Summer Sch., Univ. Antwerp*, 1973), Springer Lecture Notes in Math., **476**(1975), Table 1.
2. J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Student Texts **24**, Cambridge Univ. Press, 1991.
3. H. S. M. Coxeter & S. L. Greitzer, *Geometry Revisited*, New Math. Library **19**, Math. Assoc. of America, 1967.
4. John E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1992, Table 1.

5. Josef Gebel, Attila Pethö & Horst G. Zimmer, Computing integral points on elliptic curves, *Acta Arith.*, (to appear).
6. Richard K. Guy, The Ochoa curve, *Crux Math.*, **16**(1990) 65–69.
7. Anthony W. Knapp, *Elliptic Curves*, Math. Notes **40**, Princeton Univ. Press, 1992.
8. Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag New York, 1986.
9. Joseph H. Silverman & John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag New York, 1992.
10. Harold M. Stark, An explanation of some exotic continued fractions found by Brillhart, in Atkin & Birch (editors), *Computers in Number Theory*, (*Proc. 2nd Atlas Sympos., Oxford* (1969)), Academic Press, London, 1971, pp. 21–35.
11. Roel J. Stroeker & Nikos Tzanakis, Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arith.*, **67**(1994), 177–196.
12. Roel J. Stroeker & Benne M. M. de Weger, On elliptic diophantine equations that defy Thue—the case of the Ochoa curve, Report 9437/B, Econ. Inst., Erasmus Univ. Rotterdam, 1994 *Experimental Math.* (submitted).
13. Nikos Tzanakis & Benne M. M. de Weger, On the practical solution of the Thue equation, *J. Number Theory*, **31**(1989) 99–132; *MR* **90c**:11018.
14. Nikos Tzanakis & Benne M. M. de Weger, How to explicitly solve a Thue-Mahler equation, *Composition Math.*, **84** (1992) 223–288; *MR* **93***k*:11025; *corrections*, **89**(1993) 241–242.
15. Don Zagier, Large integral points on elliptic curves, *Math. Comput.*, **48**(1987) 425–436; *MR* **87k**:11062; Addendum, **51**(1988) 375; *MR* **89c**:11092.

Department of Mathematics & Statistics
The University of Calgary
Calgary, Alberta, CANADA T2N 1N4
rkg@cpsc.ucalgary.ca

> I have never done anything "useful". No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world ... Judged by all practical standards, the value of my mathematical life is nil; and outside mathematics it is trivial anyhow. I have just one chance of escaping a verdict of complete triviality, that I may be judged to have created something worth creating. And that I have created something is undeniable; the question is about its value.
>
> *—Godfrey H. Hardy (1877–1947)*
>
> *A Mathematician'sApology, p. 150.* Cambridge: Cambridge University Press, 1941.