Fermat's Big Problem

Keith Conrad
University of Connecticut

August 7, 2008

The Problem

In a letter from Frenicle to Fermat (1641):
Find a Pythagorean triple (a, b, c) where $a + b = \square$ and $c = \square$.

Fermat found a solution by 1643 (letter to Mersenne), which he confidently stated to be the smallest solution.

Outline

- Reduce to case $(a, b) = 1$.
- Identify with solutions of $x^4 + z^2 = 2y^4$ and side conditions.
- Solve equation using descent and ascent.

If you're willing to seek primitive solutions right away, ignore the next two slides!

Reduction to Primitive Triples

Let $g = (a, b) = (a, b, c)$, $a = ga', b = gb', c = gc'$. Then

$$\{a', b'\} = \{u^2 - v^2, 2uv\}, \quad c' = u^2 + v^2$$

with $u > v > 0$, $(u, v) = 1$, and $u \not\equiv v \bmod 2$. We will show

$$(a' + b', c') = 1.$$

Suppose a prime p divides $a' + b'$ and c'. Then $p \neq 2$ (c' is odd).

$$\begin{aligned} a' + b', c' \equiv 0 \bmod p \quad &\Rightarrow \quad u^2 - v^2 + 2uv, u^2 + v^2 \equiv 0 \bmod p \\ &\Rightarrow \quad u^2 + uv, v^2 - uv \equiv 0 \bmod p \\ &\Rightarrow \quad u(u + v), v(v - u) \equiv 0 \bmod p. \end{aligned}$$

Can't have $p|u$ and $p|v$. If $p|u$ and $p|(v - u)$ then $p|v$: NO. If $p|(u + v)$ and $p|v$ then $p|u$: NO. If $p|(u + v)$ and $p|(v - u)$ then $p|2u$ and $p|2v$, so $p|u$ and $p|v$: NO.

Reduction to Primitive Triples

Since $(a' + b', c') = 1$, $(a + b, c) = g(a' + b', c') = g$. When $a + b = \square$ and $c = \square$, $g = \square$. Thus

$$a' + b' = \frac{a + b}{g} = \square, \quad c' = \frac{c}{g} = \square.$$

So all solutions are square multiples of primitive solutions. From now on we look in $\mathbf{Z}^+$ for

$$a^2 + b^2 = c^2, \quad (a, b) = 1, \quad a + b = \square, \quad c = \square.$$

Aside: It's a Double Equation

$$a^2 + b^2 = c^2, \quad (a, b) = 1, \quad a + b = \square, \quad c = \square.$$

Then

$$\{a, b\} = \{u^2 - v^2, 2uv\}, \quad c = u^2 + v^2$$

with $u > v > 0$, $(u, v) = 1$, and $u \not\equiv v \bmod 2$, so

$$u^2 - v^2 + 2uv = \square, \quad u^2 + v^2 = \square.$$

Set $t = u/v$, in reduced form. Dividing by v^2, we get double equations

$$t^2 - 1 + 2t = \square, \quad t^2 + 1 = \square$$

with $t \in \mathbf{Q}$ and $t > 1$. Can reverse steps too, so problem is equivalent to solving double equation with rational $t > 1$.

Convert Into Quartic

We want to solve in $\mathbf{Z}^+$

$$a+b=x^2,\quad a^2+b^2=y^4,\quad (a,b)=1,\quad a \text{ odd},\quad b \text{ even}. \tag{1}$$

So $x, y \in \mathbf{Z}^+$ are odd, and

$$(a+b)^2 > a^2+b^2 \Longrightarrow x^4 > y^4 \Longrightarrow x > y > 0.$$

From the algebraic identity

$$(a+b)^2+(a-b)^2 = 2(a^2+b^2), \tag{2}$$

$x^4+(a-b)^2 = 2y^4$. Set $z = a-b$, so z is odd and

$$x^4+z^2 = 2y^4.$$

Since $(a,b)=1$ and $a \not\equiv b \bmod 2$, $(a+b, a-b)=1$, so $(x,z)=1$.

$$x^4+z^2=2y^4, (x,z)=1 \Longrightarrow (x,y)=1 \text{ and } (y,z)=1.$$

$$a+b=x^2, a-b=z \Longrightarrow 2b=x^2-z \Longrightarrow z \equiv x^2 \equiv 1 \bmod 4.$$

Convert Into Quartic

Conversely, if $x^4 + z^2 = 2y^4$ with $x, y, z \in \mathbf{Z}$ all odd and pairwise relatively prime, $x > y > 0$, and $z \equiv 1 \bmod 4$, we can solve the equations $a + b = x^2$ and $a - b = z$ for a and b:

$$a = \frac{x^2 + z}{2} \in \mathbf{Z}, \quad b = \frac{x^2 - z}{2} \in \mathbf{Z}.$$

Since $(x, z) = 1$, $(a, b) = 1$. And $a^2 + b^2 = (x^4 + z^2)/2 = y^4$. Are $a, b > 0$? Equivalent to

$$\begin{aligned} x^2 > |z| &\iff x^4 > z^2 = 2y^4 - x^4 \\ &\iff 2x^4 > 2y^4 \\ &\iff x > y. \checkmark \end{aligned}$$

Is b even? Yes: $x^2 - z \equiv 1 - z \equiv 0 \bmod 4$. So $a = b + z$ is odd.

Convert Into Quartic

Thus, we have a one-to-one correspondence between

$$a, b, x, y \in \mathbf{Z} \text{ s.t. } a+b = x^2, a^2+b^2 = y^4, (a, b) = 1, a \text{ odd}, b \text{ even}$$

and

$$\text{odd } x, y, z \in \mathbf{Z} \text{ s.t. } x^4 + z^2 = 2y^4, (x, y) = 1, z \equiv 1 \bmod 4$$

by

$$(a, b, x, y) \rightsquigarrow (x, y, a-b), \quad (x, y, z) \rightsquigarrow \left(\frac{x^2+z}{2}, \frac{x^2-z}{2}, x, y\right).$$

Moreover,

$$a, b, x, y > 0 \Longleftrightarrow x > y > 0.$$

Oddness automatic

Actually, if

$$x^4 + z^2 = 2y^4$$

with $(x, y) = 1$ then x, y, z must be odd. If y were even then x is odd and $1 + z^2 \equiv 0 \bmod 4$, which has no solution. So y is odd. Then

$$x^4 + z^2 \equiv 2 \bmod 4,$$

so x and z are both odd.
So we want to solve in $\mathbf{Z}$

$$x^4 + z^2 = 2y^4, \quad (x, y) = 1, \quad z \equiv 1 \bmod 4, \quad x > y > 0.$$

Two small solutions are $(1, 1, 1)$ and $(1, 13, -239)$, but $x \leq y$.

Descent

Suppose $x^4 + z^2 = 2y^4, (x, y) = 1, x > 0, y > 0$, and $z \equiv 1 \bmod 4$. Ignore the condition $x > y$ for now. We will find a solution (x', y', z') with $0 < y' < y$ and then write (x, y, z) in terms of (x', y', z').

Remark. It is sensible to use y as a measure of the size of (x, y, z) since the size of y controls that of x and z.

We have a Pythagorean triple:

$$x^4 + z^2 = 2y^4 \implies y^4 = \frac{x^4 + z^2}{2}$$

$$\implies (y^2)^2 = \left(\frac{x^2 + z}{2}\right)^2 + \left(\frac{x^2 - z}{2}\right)^2.$$

Could $x^2 = \pm z$? Then $2x^4 = 2y^4 \Rightarrow x = y = 1$. So when $y > 1$, $x^2 \neq \pm z$.

Descent

$$(y^2)^2 = \left(\frac{x^2+z}{2}\right)^2 + \left(\frac{x^2-z}{2}\right)^2, \quad y^2 > 1.$$

Since x is odd and $z \equiv 1 \bmod 4$, $(x^2-z)/2$ is even. The parametric formula for nonzero triples (maybe $(x^2 \pm z)/2 < 0$) says

$$\frac{x^2+z}{2} = u^2 - v^2, \quad \frac{x^2-z}{2} = 2uv, \quad y^2 = u^2 + v^2,$$

for $u, v \in \mathbf{Z} - \{0\}$, $(u, v) = 1$, $u \not\equiv v \bmod 2$. Add and subtract:,

$$x^2 = u^2 - v^2 + 2uv = (u+v)^2 - 2v^2$$

and

$$z = u^2 - v^2 - 2uv \Longrightarrow 1 \equiv u^2 - v^2 \bmod 4,$$

so u is odd and v is even. No effect in formulas by $(u, v) \mapsto (-u, -v)$. So (for later purposes) we may suppose

$$u + v > 0.$$

Descent

So far

$$x^2 = (u+v)^2 - 2v^2, \quad y^2 = u^2 + v^2, \quad z = u^2 - v^2 - 2uv,$$

where $(u, v) = 1$, u odd, v even (not 0). Because $y^2 = u^2 + v^2$ with $(u, v) = 1$, v is even, and $y > 0$, the parametric formula for nonzero triples says

$$u = k^2 - \ell^2, \quad v = 2k\ell, \quad y = k^2 + \ell^2,$$

where $k, \ell \in \mathbf{Z} - \{0\}$, $(k, \ell) = 1, k \not\equiv \ell \bmod 2$. Therefore

$$u + v = k^2 - \ell^2 + 2k\ell.$$

No effect by $(k, \ell) \mapsto (-k, -\ell)$, so may suppose $k > 0$. We will use $x^2 = (u+v)^2 - 2v^2$ to get second formulas for $u + v$ and v.

Descent

$$x^2 = (u+v)^2 - 2v^2 \Longrightarrow x^2 + 2v^2 = (u+v)^2,$$

with $(u, v) = 1$, u odd, v even.

Theorem

The solutions (A, B, C) to $A^2 + 2B^2 = C^2$ in $\mathbf{Z}^+$ with $(A, B) = 1$ are given by

$$A = |t^2 - 2w^2|, \quad B = 2tw, \quad C = t^2 + 2w^2,$$

where $t, w > 0$, $(t, w) = 1$, and t is odd.

Thus

$$x = |t^2 - 2w^2|, \quad |v| = 2tw, \quad |u+v| = t^2 + 2w^2.$$

with $t > 0$ odd. Choose the sign on w so $v = 2tw$. Since $u + v > 0$, $u + v = t^2 + 2w^2$.

Descent

We now have two formulas for $u+v$ and for v:

$$u+v = k^2 - \ell^2 + 2k\ell, \quad u+v = t^2 + 2w^2$$

$$v = 2k\ell, \quad v = 2tw.$$

And

$$x = |t^2 - 2w^2|, \quad y = k^2 + \ell^2, \quad z = u^2 - v^2 - 2uv.$$

From the two v-formulas, $k\ell = tw$, and recall $k > 0$, $t > 0$, so

$$\frac{k}{t} = \frac{w}{\ell} =: \frac{y'}{x'} \text{ with } x' > 0, y' > 0, (x', y') = 1.$$

Thus

$$k = y'\lambda, \quad t = x'\lambda, \quad w = y'\mu, \quad \ell = x'\mu$$

for some $\lambda \in \mathbf{Z}^+$ and $\mu \in \mathbf{Z} - \{0\}$. Since $(k, \ell) = 1$, $(\lambda, \mu) = 1$.

Descent

From

$$u + v = k^2 - \ell^2 + 2k\ell, \quad u + v = t^2 + 2w^2$$

and

$$k = y'\lambda, \quad t = x'\lambda, \quad w = y'\mu, \quad \ell = x'\mu,$$

we will get a quadratic with root μ/λ:

$$\begin{aligned} (y'\lambda)^2 - (x'\mu)^2 + 2x'y'\lambda\mu &= (x'\lambda)^2 + 2(y'\mu)^2 \\ y'^2\lambda^2 + 2x'y'\lambda\mu &= x'^2\lambda^2 + (x'^2 + 2y'^2)\mu^2. \end{aligned}$$

Divide by λ^2 and rearrange into quadratic in μ/λ:

$$0 = (x'^2 + 2y'^2)\left(\frac{\mu}{\lambda}\right)^2 - 2x'y'\left(\frac{\mu}{\lambda}\right) + (x'^2 - y'^2).$$

Having a rational root μ/λ, the discriminant is a perfect square:

$$(2x'y')^2 - 4(x'^2 + 2y'^2)(x'^2 - y'^2) = 4(2y'^4 - x'^4) \stackrel{!}{=} \square.$$

Descent

So $2y'^4 - x'^4 = z'^2$ for some $z' \in \mathbf{Z}$: $x'^4 + z'^2 = 2y'^4$. From $(x', y') = 1$, x', y', z' are all (automatically) odd. Choose the sign on z' so $z' \equiv 1 \bmod 4$.
Applying quadratic formula to

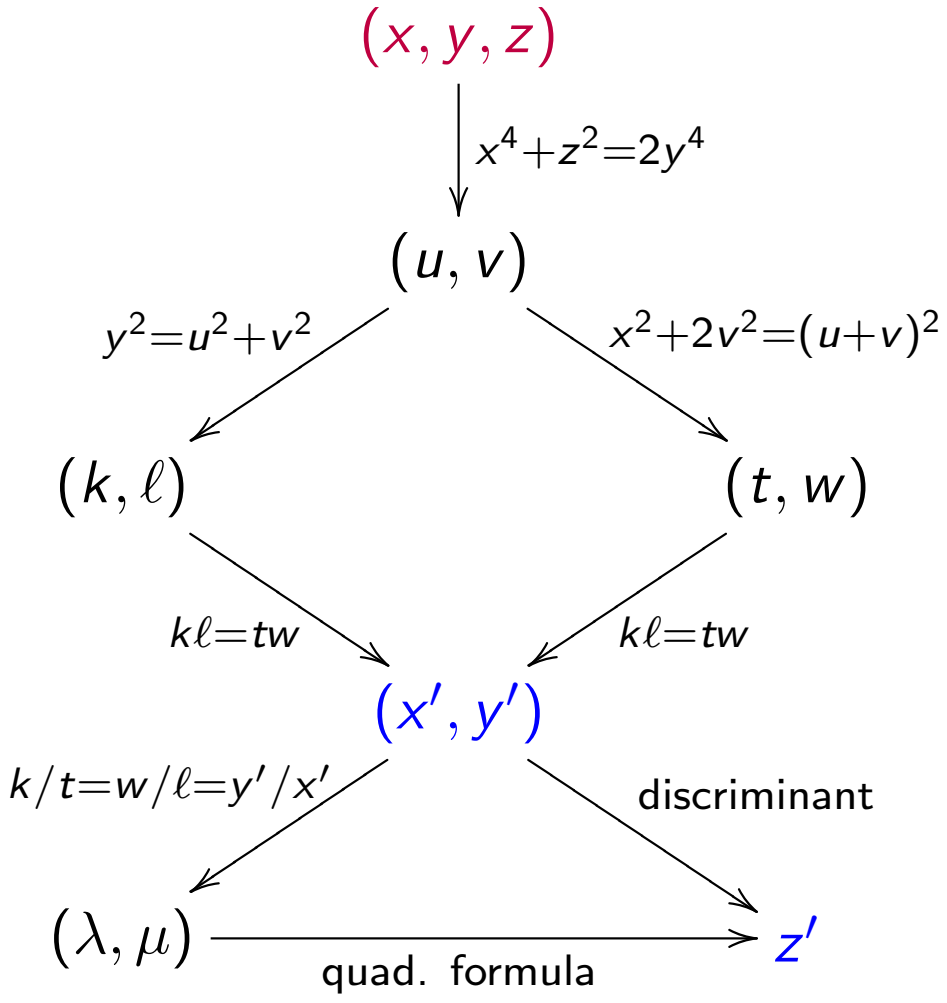
$$0 = (x'^2 + 2y'^2)\left(\frac{\mu}{\lambda}\right)^2 - 2x'y'\left(\frac{\mu}{\lambda}\right) + (x'^2 - y'^2)$$

gives us

$$0 \neq \frac{\mu}{\lambda} = \frac{2x'y' \pm \sqrt{4z'^2}}{2(x'^2 + 2y'^2)} = \frac{x'y' \pm z'}{x'^2 + 2y'^2}.$$

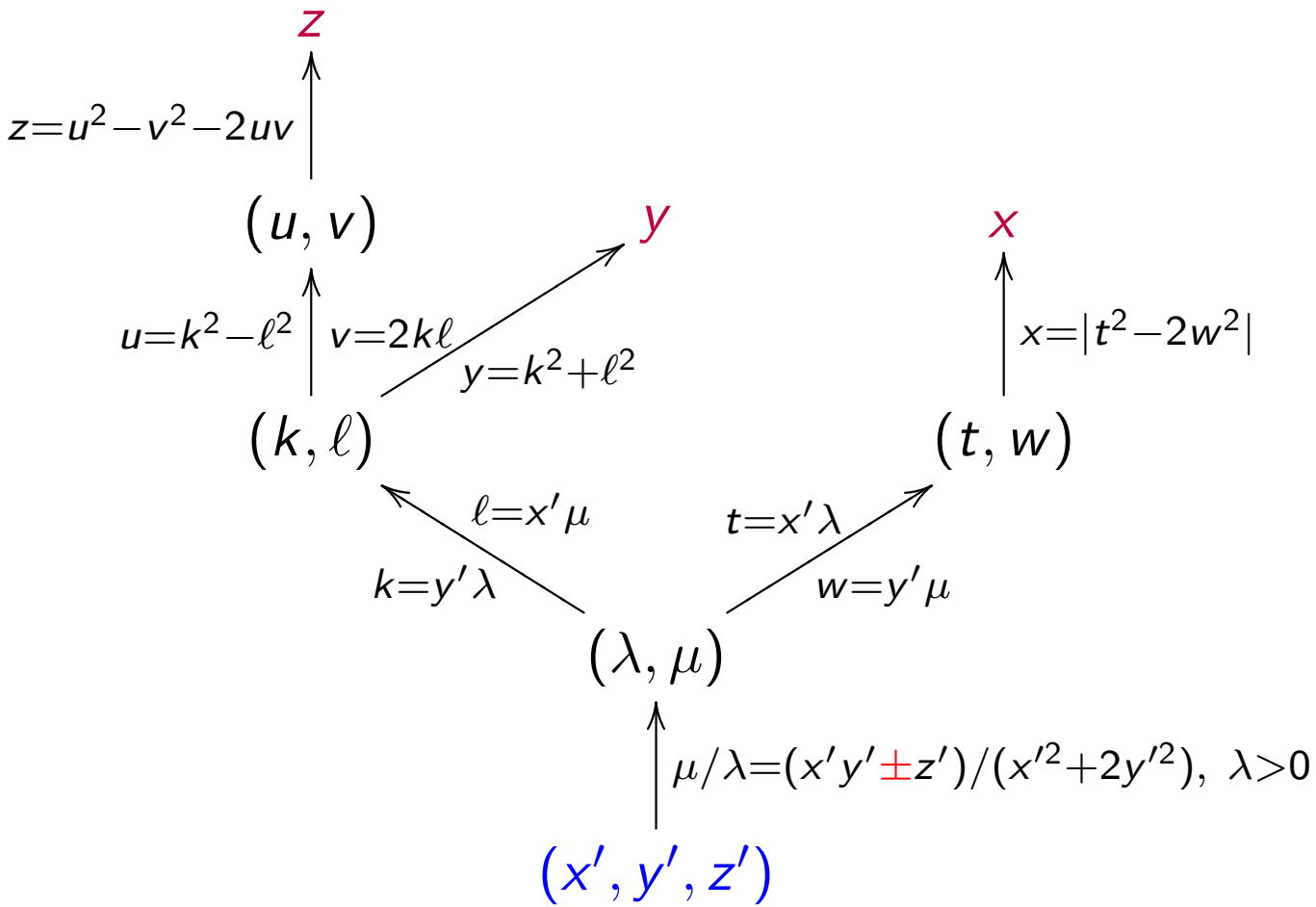
Since $y = k^2 + \ell^2 = (y'\lambda)^2 + (x'\mu)^2 > y'^2 \geq y'$, we have $0 < y' < y$, so $(x, y, z) \rightsquigarrow (x', y', z')$ is a descent.

Descent Schematic



Descending enough times eventually brings us down to $(1, 1, 1)$.

Ascent Schematic



Ascent

Suppose x', y', z' in $\mathbf{Z}$ satisfy $x'^4 + z'^2 = 2y'^4$ with $(x', y', z') = 1$, $x' > 0$, $y' > 0$, and $z' \equiv 1 \bmod 4$. Then $x^4 + z^2 = y^4$ with $(x, y, z) = 1$, $x > 0, y > 0$, and $z \equiv 1 \bmod 4$.
So all such solutions (x, y, z) can be found by ascent from $(1, 1, 1)$.
Let's ascend until we reach an (x, y, z) with $x > y$, which is the criterion corresponding to a right triangle.

Ascent : Check When $x > y$

x'	1	1	1	1
y'	1	1	13	13
z'	1	1	-239	-239
sign	$+$	$-$	$+$	$-$
μ	2	0	-2	84
λ	3	X	3	113
k	3		39	1469
ℓ	2		-2	84
w	2		-26	1092
t	3		3	113
u	5		1517	2150905
v	12		-156	246792
x	1		1343	2372159
y	13		1525	2165017
z	-239		2750257	3503833734241

Fermat's Solution To His Big Problem!

$$(x, y, z) = (2372159, 2165017, 3503833734241)$$

$$a = \frac{x^2 + z}{2} = 4565486027761$$

$$b = \frac{x^2 - z}{2} = 1061652293520$$

$$c = y^2 = 4687298610289$$

$$a + b = x^2 = (2372159)^2, \quad c = y^2 = (2165017)^2.$$

Fermat expected this solution (where a, b, and c have 13 digits each) is smallest. Could $(1343, 1525, 2750257)$ ascend to (x, y, z) with $y < 2165017$? Let's go back to the table!

Ascent : Check When $x > y$

x'	1343
y'	1525
z'	2750257
sign	$+$
μ	84
λ	113
k	172325
ℓ	112812
w	128100
t	151759
u	16969358281
v	38880655800
x	9788425919
y	42422452969
z	-2543305831910011724639

Ascent : Check When $x > y$

x'	1343
y'	1525
z'	2750257
sign	$-$
μ	-6214
λ	57123
k	87112575
ℓ	-8345402
w	-9476350
t	76716189
u	751895498858902 1
v	$-145397891526030 0$
x	570577123603872 1
y	765824645767222 9
z	762854334708055785041475599810 41

Ascent : Check When $x > y$

x'	2372159
y'	2165017
z'	3503833734241
sign	$+$
μ	151245528
λ	262621633
x	1736585395538252121495132514 57
y	45200552689788884429350416 5425
z	$-$28735843459830450828532552 8722
	58900270264570574287338609 4143

Ascent : Check When $x > y$

x'	2372159
y'	2165017
z'	3503833734241
sign	$-$
μ	6214
λ	57123
x	17999572487701067948161
y	15512114571284835412957
z	10409335321015716539793
	0031823738667393894481

Second Solution and Second Triangle

$$
\begin{aligned}
x &= 1799957248770106794816 1 \\
y &= 15512114571284835412957 \\
z &= 10409335321015716539793 \\
&\quad 003182373866739389448 1 \\
a &= 21403898147508118863494704189224 \\
&\quad 5670988588201 \\
b &= 10994562826492402323701701006850 \\
&\quad 7003594693720 \\
c &= 24062569847266731316041529500536 \\
&\quad 8384723483849
\end{aligned}
$$

Here $a + b = x^2$ and $c = y^2$. Sides of triangle are 45 digits each.

Third Triangle

$$
\begin{aligned}
a &= 10109044591231561118979763310306 \\
&\quad 22692818310726588504638143451555 \\
&\quad 19536067859788318450595485833321 \\
b &= 90600415152500364825256074903956 \\
&\quad 70080369538218738625798135550122 \\
&\quad 18954815260263533071161286620 0 \\
c &= 13574871447109996764509830381541 \\
&\quad 31451835106044687792312854628713 \\
&\quad 41558087008619938117875754653321
\end{aligned}
$$

Here a has 96 digits, b has 95, and c has 96.

Fourth Triangle (165 digits per side)

$$
\begin{aligned}
a &= 463364435981466638655721606795402574490785034897443124170070240200671104946933926803365302534576258476492322816713177661024808525677009601280034178493297316385999153\\
b &= 704093322799308833776272853814930313676549030172246816105298509194049219955867268919807417417483602815295710263978203420907943571429370020707878980026592034112342096\\
c &= 842884338294996678212228837815191418234428179249675666444859533148402499591532256435242317441040296075151069741561268252863830134704359471711958336290700625845640625
\end{aligned}
$$

Fifth Triangle's Legs (254 digits per side)

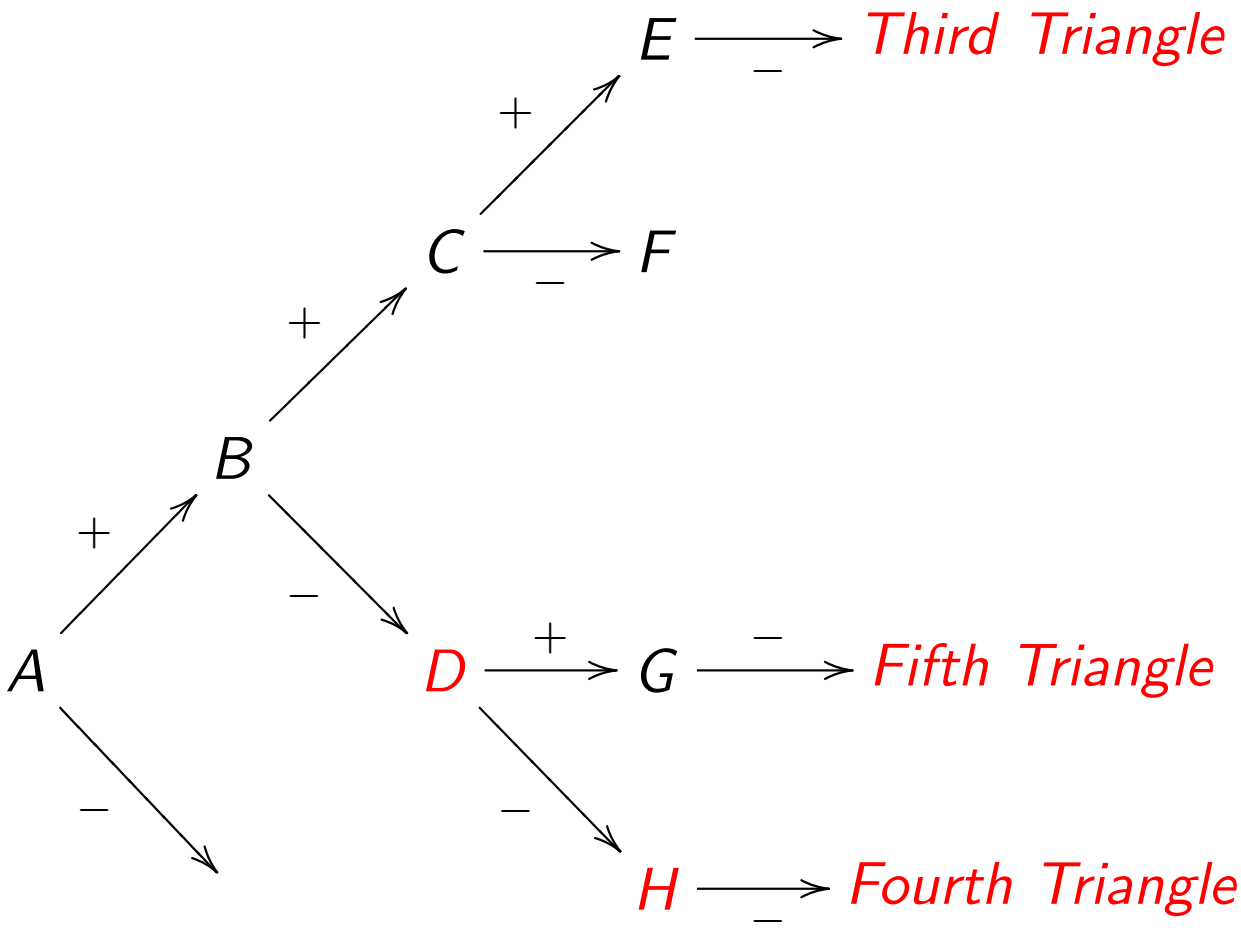
$$
\begin{aligned}
a = {} & 18693892687943762664743001838718605462225799 \\
& 08983368632811550970905602722938264699292786 \\
& 97338089732313774867405929869284850781681454 \\
& 98290629949354665422452699662399182593359518 \\
& 03493122671390234659552729218724304820963551 \\
& 17152584741062173732896154998755 21 \\
b = {} & 54446069896073289936866119261148374495685470 \\
& 06847048907950413644850398418560240884778914 \\
& 27640633937043249562546629831881335518716487 \\
& 43263231336259210670711763511827361741373381 \\
& 51097989105474592489720710882472950462110102 \\
& 65311717123372074776983570606032 00
\end{aligned}
$$

Fifth Triangle's Hypotenuse (254 digits per sides)

$$
\begin{aligned}
c &= 57565928733552587623450413523345988485082828 \\
&\quad 36770355044269203170071305751820346779650053 \\
&\quad 88776940832138172675658879288033121595186569 \\
&\quad 43218470008771005269705652554396832114307802 \\
&\quad 88785893181066054985482449842902616011177690 \\
&\quad 33321056678710537574731478505955 21 \\
a+b &= 85521905137816622777331086089800761983566959 \\
&\quad 68757207916596240017847167622940912552801901 \\
&\quad 941540265544444243455618939832244637439^2 \\
c &= 75872214106056367032449378399666730949102564 \\
&\quad 00181651173720177950441604458933137545365325 \\
&\quad 56172179231760522364174622647110490428 9^2
\end{aligned}
$$

Ascent Diagram

Label solutions to $x^4 + z^2 = 2y^4$ in the order above alphabetically, so $A = (1, 1, 1)$, $B = (1, 13, -239)$, and so on.



Link to Elliptic Curves

$$x^4 + z^2 = 2y^4, \quad (x, y) = 1 \Longrightarrow 1 + \left(\frac{z}{x^2}\right)^2 = 2\left(\frac{y}{x}\right)^4.$$

Conversely, if $1 + v^2 = 2u^4$ in $\mathbf{Q}$, write $u = y/x$ in reduced form. Then multiply through by x^4: $x^4 + x^4v^2 = 2y^4$, so

$$x^4v^2 \in \mathbf{Z} \Longrightarrow (x^2v)^2 \in \mathbf{Z} \Longrightarrow x^2v \in \mathbf{Z}.$$

Set $z = x^2v$, so $u = y/x$ and $v = z/x^2$. The condition $x > y > 0$ for having a right triangle corresponds to $0 < u < 1$.
For positive rational solutions,

$$\begin{aligned} 2v^2 = u^4 + 1 &\iff (u, v) = (1, 1), \\ 2v^2 = u^4 - 1 &\iff \text{NONE}, \\ v^2 = 2u^4 - 1 &\iff (u, v) = (1, 1), (13, 239), \ldots \end{aligned}$$

Link to Elliptic Curves

There is essentially a one-to-one correspondence between points on $v^2 = 2u^4 - 1$ and $Y^2 = X^3 + 8X$:

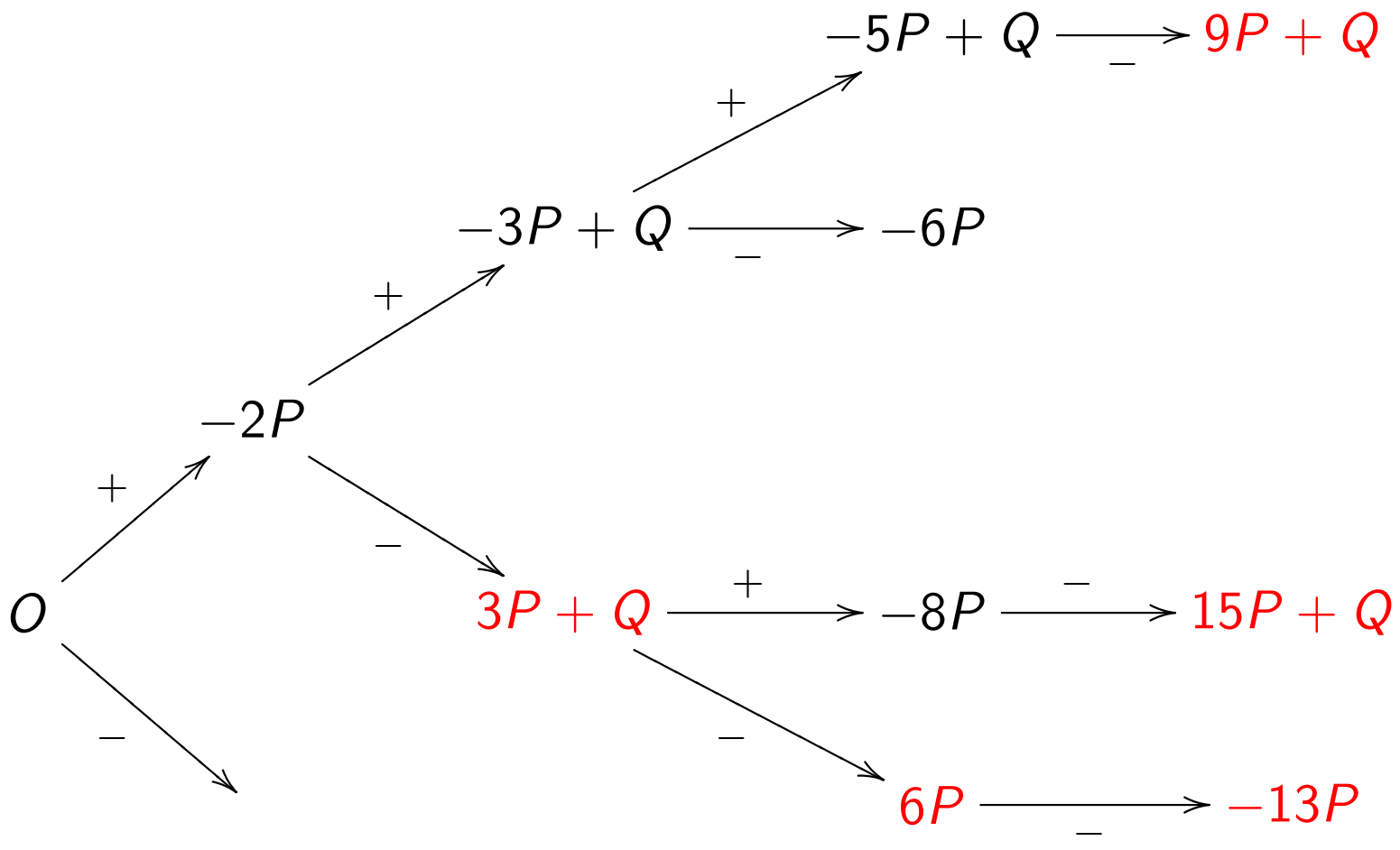
$$X = \frac{2(v + 2u^2 - 1)}{(u-1)^2} \qquad Y = \frac{4(2u^3 + (2u-1)v - 1)}{(u-1)^3},$$

$$u = \frac{Y - 2X - 8}{Y - 4X + 8} \qquad v = \frac{Y^2 - 24X^2 + 48Y - 16X - 64}{(Y - 4X + 8)^2}.$$

The group of rational points on $Y^2 = X^3 + 8X$ has the form $\langle (0,0), (1,3) \rangle$, where $(0,0)$ has order 2 and $(1,3)$ has infinite order. Also the group is $\langle (0,0), (0,0) - (1,3) \rangle = \langle (0,0), (8,24) \rangle$. Compare with $\mathbf{Z}[\sqrt{2}]^\times = \langle -1, 1 + \sqrt{2} \rangle = \langle -1, 1 - \sqrt{2} \rangle$, where $1 - \sqrt{2} = -(1 + \sqrt{2})^{-1}$.

Ascent in Terms of $Y^2 = X^3 + 8X$

Let $P = (8, 24)$ and $Q = (0, 0)$.



Redoing Ascent

Recall ascent formulas.
If x', y', z' in $\mathbf{Z}$ satisfy $x'^4 + z'^2 = 2y'^4$ with $(x', y', z') = 1$, write

$$\frac{\mu}{\lambda} = \text{reduced form of } \frac{x'y' \pm z'}{x'^2 + 2y'^2}, \quad \lambda > 0.$$

Allow both sign choices. Set

$$k = y'\lambda, \quad t = x'\lambda, \quad w = y'\mu, \quad \ell = x'\mu,$$

$$u = k^2 - \ell^2, v = 2k\ell, x = |t^2 - 2w^2|, y = k^2 + \ell^2, z = u^2 - v^2 - 2uv.$$

The absolute value arises from the motivating problem. Let's remove it and use $x = t^2 - 2w^2$. What does this mean in terms of ascent on the elliptic curve?

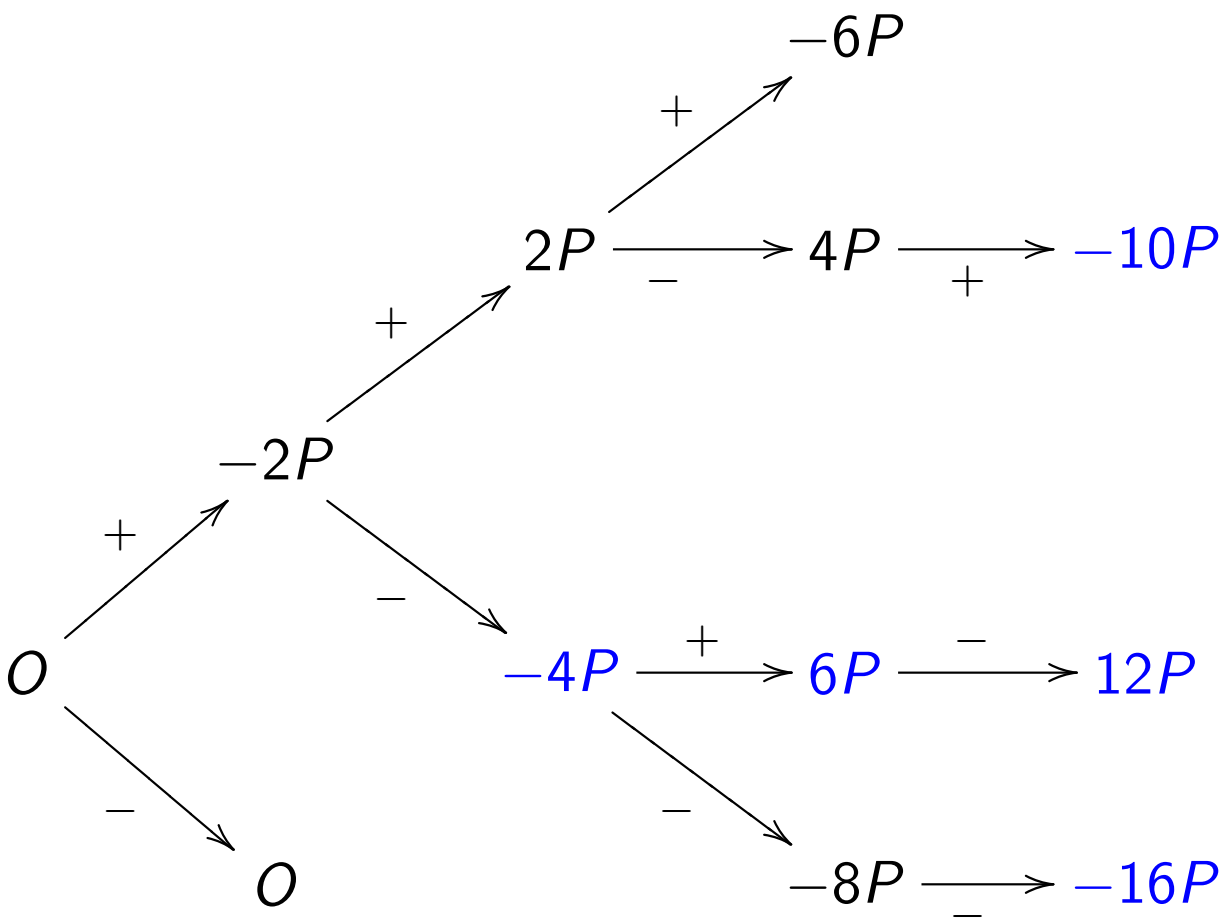
Redoing Ascent

x'	1	1	1	1
y'	1	1	13	13
z'	1	1	-239	-239
sign	$+$	$-$	$+$	$-$
μ	2	0	-2	84
λ	3	X	3	113
x	1		-1343	-2372159
y	13		1525	2165017
z	-239		2750257	3503822734241

New ascent of $(-1343, \ldots, +)$ is old ascent of $(1343, \ldots, -)$,
New ascent of $(-1343, \ldots, -)$ is old ascent of $(1343, \ldots, +)$,
N. A. of $(-2372159, \ldots, +)$ is O.A. of $(2372159, \ldots, -)$,
N. A. of $(-2372159, \ldots, -)$ is O.A. of $(2372159, \ldots, +)$,

Redoing Ascent on $Y^2 = X^3 + 8X$

Let $P = (8, 24)$, $Q = (0, 0)$. Ascents are $R \xrightarrow{+} -2R - 2P$, $R \xrightarrow{-} 2R$.



Triangles in order correspond to $-4P, 6P, -10P, 12P, -16P, \ldots$.