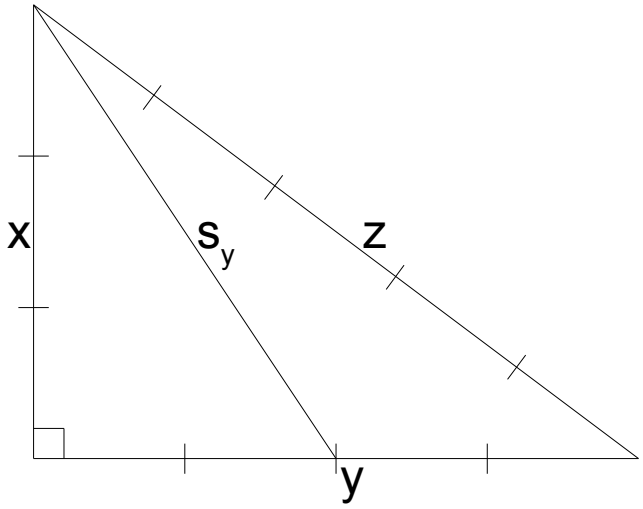
Ralf Steiner 16-20.09.2020

Zur Seitenhalbierenden der geraden Kathete eines pPT sowie zu den Primzahlen der Form p≡1 (mod 12).



Bei einem primitiven pythagoreischen Dreieck pPT(x,y,z) mit $x^2+y^2=z^2$ sei x die ungerade und y die gerade Kathete. Dann ist y/2 stets ganz. Die y-Seitenhalbierende s_y genügt somit der pythagoreischen Gleichung: $x^2+(y/2)^2=s_y^2$. Die Summe zweier Quadratzahlen (davon zumindest eine ungerade) ist im Allgemeinen nicht notwendig eine Quadratzahl, so ist wie in obiger Figur dargestellt bspw. s_y^2 von pPT(3,4,5) gleich $3^2+(4/2)^2=13\equiv1$ (mod 12) kein Quadrat und somit s_y eine irrationale Quadratwurzel.

Satz: Für pythagoreische Dreiecke pPT(x,y,z), y gerade gilt für die y-Seitenhalbierende s_y:

1) s_y ist eine irrationale Quadratwurzel;
2) s_y^2 besteht nur aus (vielfachen) Primfaktoren p_i mit $p_i \equiv1$ (mod 12);
3) $s_y^2 \equiv1$ (mod 12).

Beweise

1)

Angenommen s_y wäre rational, dann würde $s_y=p/q$ gelten mit p,q aus $\mathbb{N}$ kleinstmöglich und teilerfremd. Dann ist $s_y^2=p^2/q^2=x^2+(y/2)^2$ also ganzzahlig $p^2=q^2x^2+q^2y^2/4=(qx)^2+(qy/2)^2$ $=q^2(x^2+(y/2)^2)$ sowie mit quadratischer Ergänzung $(p/q)^2+xy=(x+y/2)^2$ bzw. ganzzahlig $p^2+q^2xy=q^2(x+y/2)^2$.

Falls q gerade und p ungerade (sowie da y gerade und x ungerade) wäre die linke Seite p^2+q^2xy als Summe eines ungeraden und eines geraden Summanden ungerade, die rechte Seite $q^2(x+y/2)^2$ aber gerade durch geraden Faktor, was nicht möglich ist.
Somit ist p gerade und q ungerade (sowie da y gerade und x ungerade) und die linke Seite als Summe zweier gerader Summanden gerade, wodurch auf der rechten Seite der Faktor (x+y/2) gerade sein muss. Dazu muss y/2 ungerade und somit darf 4 kein Teiler von y sein, also ist y=2k=2i+1 mit k ungerade. Dann ist auch im notwendig geraden Faktor $(x^2+(y/2)^2)$ der notwendig ungerade Summand $(y/2)^2=k^2=(2i+1)^2$. Die Summe zweier teilerfremder ungerader Quadrate ist jedoch niemals ein Quadrat, da in jedem pPT(x,k,p/q) stets zumindest eine Kathete gerade ist. Die Wurzel des Terms $(x^2+(2i+1)^2)$ ist somit notwendig irrational und damit $p/q=\sqrt{(x^2+(2i+1)^2)}$. Damit ist 1) bewiesen.

2)

Es existiert mit pPT(3,4,5) und der Fläche $A=xy/2=3\cdot4/2=6$ eine Seitenhalbierende $s_y^2=3^2+2^2=13\equiv1 \pmod{12}$, welche nach dem Strahlensatz die Fläche halbiert. Da nach 1) die Seitenhalbierende s_y stets irrational ist kann jedoch ein (nicht notwendig primitives) $PT(x,y/2,s_y)$ mit der Fläche $A=xy/2/2=3\cdot4/2/2=3$ nicht existieren.

Angenommen s_y^2 würde aus Primfaktoren p_i, q_i aus P bestehen, wobei die $1<p_i$ jeweils der Form $p_i \equiv1 \pmod{12}$ jedoch die $1<q_i$ jeweils nicht der Form $q_i \equiv1 \pmod{12}$ genügen, also $s_y^2=pq=x^2+(y/2)^2$ mit $p=\prod p_i$ und $q=\prod q_i$ (je mehrfach gezählt). Zudem sei bei pPT(x,y,z), x,y<z paarweise teilerfremd das y gerade.

Sei $k=y/2=2i+1$ ungerade (4 teilt y nicht) und somit $pq=x^2+k^2=x^2+(2i+1)^2$ die Summe zweier ungerader Quadrate, welche gerade ist. Allerdings gibt es kein solches pPT(x,2(2i+1),z), da x,z stets ungerade sowie teilerfremd sind aber eine Kathete eines pPT durch 4 teilbar sein muss.

Also sei $k=y/2=2i$ gerade (also 4|y) und somit $pq=x^2+k^2=x^2+4i^2$die Summe eines ungeraden und eines geraden Quadrats, welche ungerade ist. Da p ungerade ist muss auch q ungerade sein (also kein Primfaktor 2 in q auftreten) und somit ist pq ungerade. Mit $y^2=(y/2)^2+3(y/2)^2$ in $z^2=x^2+y^2=pq+3k^2=pq+12i^2$ eingesetzt ist sowohl die linke Seite ungerade als auch die rechte Seite als Summe eines ungeraden und eines geraden Summanden.

Mit Euklids Formeln lässt sich jedes pPT(x,y,z) eindeutig als pPT(u,v) darstellen, mit $x=u^2-v^2$, $y=2uv$, $z=u^2+v^2$, $ggT(u,v)=1$, $u-v\neq1 \bmod 2$. Dies ergibt $(u^2+v^2)^2=4u^2v^2+(u^2-v^2)^2=12(uv/2)^2+pq$ und somit $(u^2+v^2)^2=u^4-u^2v^2+v^4$. Letzterer Term $u^4-u^2v^2+v^4=pq$ ist zwar in $\mathbb{R}$ nicht allgemein in pq faktorisierbar, wohl aber in $\mathbb{C}$ mit $(u^2-iuv-v^2)(u^2+iuv-v^2)$, $i^2=-1$ sowie als $(u^2+v^2)^2 \bmod 3$ sowie $(u^2+uv+v^2)^2 \bmod 2$.

Der in der Gleichung auftretende Faktor 12 impliziert eine Betrachtung mod 12: $(u^2+v^2)^2\equiv 0u^2v^2+(u^2-v^2)^2\equiv0(uv/2)^2+1q \pmod{12}$, wobei aus $1q \equiv1 \pmod{12}$ mit dem Chinesischen Restsatz zudem jeweils folgt: $1q\equiv1 \pmod 3$ und $1q\equiv1 \pmod 4$ sowie $1q\equiv1 \pmod 2$ und $1q\equiv1 \pmod 6$. Da $(u^2+v^2)^2\equiv(u^2-v^2)^2\equiv1q \pmod{12}$ für alle zulässigen $0<v<u$ gelten muss folgt $q=1$. Also treten mit $q=1=\prod q_i$ keine q_i auf. Somit ist $s_y^2=p=\prod p_i$. Damit ist 2) bewiesen.

3)

Aus 2) folgt $s_y^2=p=\prod p_i$ mit $p_i\equiv1 \pmod{12}$. Da $(a \bmod m \cdot b \bmod m) \bmod m = a\cdot b \bmod m$ gilt, folgt daraus $s_y^2=\prod p_i \equiv1 \pmod{12}$. Damit ist 3) bewiesen.

Mit den Teilbeweisen zu 1), 2) und 3) ist obiger Satz bewiesen. Q.E.D.

Korollar

Es existiert bei jedem pPT(x,y,z) zudem auch je eine y-Seitenviertelnde s_{y14} sowie eine y-Seitendreiviertelnde s_{y34}. Analoge Betrachtungen führen zu Aussagen:
1) s_{y14} und s_{y34} sind irrationale Quadratwurzeln;
2) s_{y14}^2 besteht aus Primfaktoren $\{2,1 \bmod 4\}$, s_{y34}^2 besteht aus Primfaktoren $\{2,3,1 \bmod 4\}$;
3) s_{y14}^2 ist eine Zweierpotenz (inkl.2^0) von 1 mod 4,
   s_{y34}^2 ist eine Zweierpotenz (inkl.2^0) mal einer Dreierpotenz (inkl.3^0) von 1 mod 4.