MULTIPLE PYTHAGOREAN NUMBER TRIPLES

By

Albert Fässler

IMA Preprint Series # 438

August 1988

MULTIPLE PYTHAGOREAN NUMBER TRIPLES

ALBERT FÄSSLER*

Abstract. We focus on the following questions: How many pythagorean number triples, whose triangles have a common hypothenuse, legsum, legdifference, area, perimeter, inradius or leg do exist, if any, and how can they be calculated? How are such triples distributed for small parameters as well as asymtotically? Some statistical and graphical representations generated with the computer will be represented. Asymtotical statements might appear as a surprise for someone not very familiar with number theory. In Section 3, a new, short and from the algorithmic point of view constructive geometrical proof for Lemma 2 will be given. A survey of published result is integrated in this article with some historical remarks, to make it an enjoyable reading.

1. Introduction.

A triple of strictly positive integers x, y, h satisfying

$$x^2 + y^2 = h^2 \tag{1.1}$$

is called a *Pythagorean number triple*, or shorter a *Pythagorean triple*.

A pythagorean triple, shortly denoted by $[x, y, h]$, is called *primitive* iff x, y, h are relatively prime, i.e. their gcd is 1; it is sufficient, that $gcd(x, y) = 1$ holds.

Because x and y both odd would imply $h^2 \equiv 2 \pmod 2$, which is impossible, one leg has to be even and one leg has to be odd. At least known since Euclid is the following way of discribing the primitive pythagorean triples (short notation ppt):

The pairs of integers [a,b] with the properties

$$a > b > 0 \qquad gcd(a, b) = 1 \qquad a + b \equiv 1 \pmod 2 \tag{1.2}$$

generate the set of all ppt $[x, y, h]$ with x even and y odd by

$$x = 2ab \qquad y = a^2 - b^2 \qquad h = a^2 + b^2 \tag{1.3}$$

The above description is a *bijection* between the pairs $[a, b]$ with properties (1.2) and all the ppt $[x, y, h]$ with x even.

If we choose any pair $a > b > 0$, we still would get pythagorean triples by (1.3), but they would not be primitive in general.
We call a and b *generators* of the primitive triple $[x, y, h]$.

Examples.

$$[2,1] \longleftrightarrow [4,3,5] \qquad [3,2] \longleftrightarrow [12,5,13] \qquad [21,4] \longleftrightarrow [168,425,457]$$

*Institute for Mathematics and its Applications, University of Minnesota, Minneapolis, MN 55455 U.S.A. and Ingenieurschule Biel, Postfach 1180, CH-2500 Biel/Bienne Switzerland. This work was mainly done when the author was spending his sabbatical leave in Minneapolis. He wishes to thank the State of Bern in Switzerland for its support and the IMA at the University of Minnesota for its provisions of excellent working conditions and computer facilities.

GEOMETRIZATION.

(1.3) can be considered as the conformal mapping $z \mapsto z^2$ with $z = a + ib$:

$$(a+ib)^2 = (a^2 - b^2) + i \cdot 2ab \tag{1.4}$$

Indeed, $y = Re(z^2)$ and $x = Im(z^2)$. Introducing axis of coordinates as shown in Fig. 1, the mapping $z \mapsto z^2$, in a first step discussed for the entire (a,b)–plane, has the following properties:

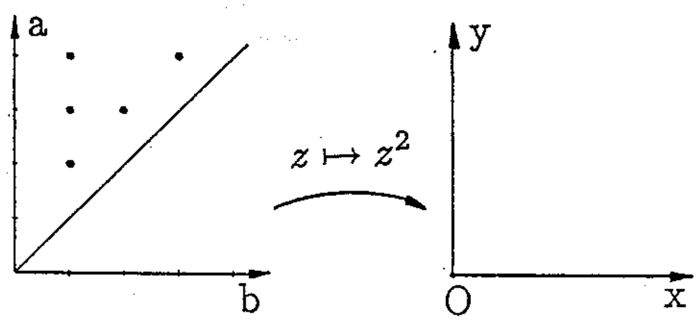

Fig. 1

For $a = a_0 = \text{const}$, we get $y = a_0^2 - b^2$ and $x = 2a_0 b$ which for $a_0 \neq 0$ implies $b = x/2a_0$, and particularly

$$y = -\frac{x^2}{4a_0^2} + a_0^2 \tag{1.5}$$

Therefore the images of horizontal lines are parabolas symmetric about the y-axis with the common foci in the origin O and open downwards, the exeptional case $a_0 = 0$ gives us as image the negative part of the y–axis.

Similarly, the images for vertical lines $b = b_0 = \text{const}$ are described by

$$y = \frac{x^2}{4b_0^2} - b_0^2 \quad , \qquad b_0 \neq 0 \tag{1.6}$$

and therefore are parabolas as mentioned before, but open upwards.

Images restricted to $a \geqq b \geqq 0$ (see Fig. 1) lie in the first quadrant. Furthermore, $y = 0$ implies $x^2 = 4a_0^4$ resp. $x^2 = 4b_0^4$. Therefore, parabolas of the two orthogonal families have a point on the positive x–axis in common iff $a_0 = b_0$.

Fig. 2 shows the images for curves with $a = 1, 2, 3, \cdots, 42$ and $b = 1, 2, 3, \cdots, 30$. In particular, the computer generated points mark *all* the ppt in the range x and $y \lessapprox 1800$, where the distance from the origin to such a point gives the length of the hypothenuse for the corresponding right triangle.

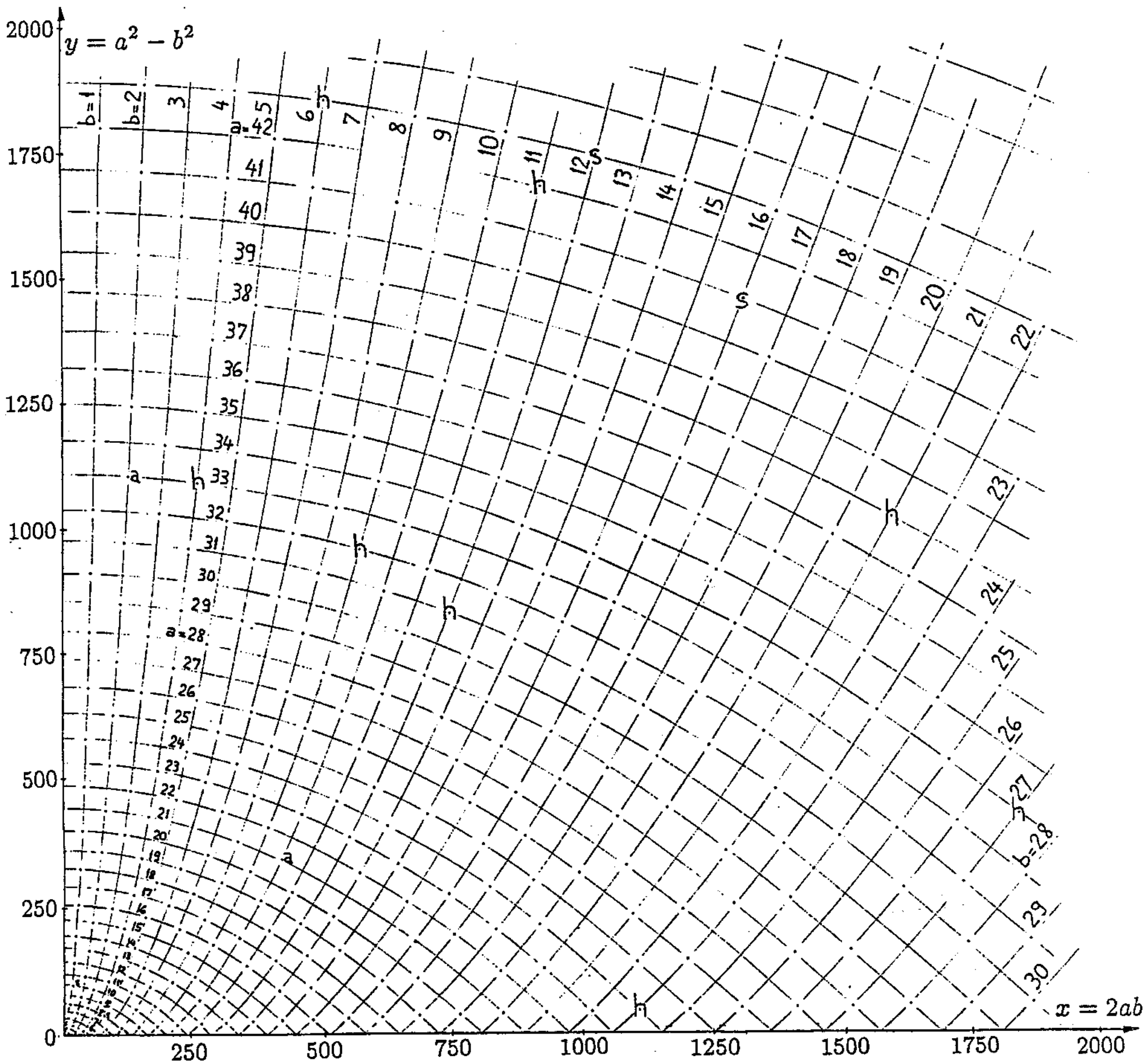

Fig. 2

Note,that

$$\text{(1.7)} \qquad \#\text{ of points on a curve with const a–value} = \begin{cases} \varphi(a) & \text{if a is even} \\ \varphi(a)/2 & \text{if a is odd} \end{cases}$$

where $\varphi(a) = \#$ of positive integers less than a and relatively prime to a. φ is called *Euler– function*. If a is even, (1.7) holds by definition. If a is odd, we know that $gcd(a,k) = gcd(a,a-k)$. But a and $a-k$ have different parity, i.e. their sum is odd. Therefore exactly one of a pair $a, a-k$ is even.

If by reflexion with reference to the axis $x = y$ in Fig. 2, we map all the points with $y > x$ into the domain $x > y > 0$, we get Fig. 3. The density of ppt has doubled in releasing that x has to be even, however we lost the nice geometrical pattern.

Fig. 3

GUIDELINE OF THIS ARTICLE. *We focus on the following questions: How many pythagorean number triples, whose triangles have a common hypothenuse,legsum, legdifference, area, perimeter, inradius or leg do exist, if any, and how can they be calculated? How are such triples distributed for small parameters as well as asymtotically? Some statistical and graphical representations generated with the computer will be represented. Asymtotical statements might appear as a surprise for someone not very familiar with number theory. In Section 3, a new, short and from the algorithmic point of view constructive geometrical proof for Lemma 2 will be given. A survey of published results and historical remarks are integrated to make this article an enjoyable reading.*

Some corresponding points to primitive multiple triples with common hypothenuse in Fig. 2 are marked with h. Similarly, *s* holds for a common legsum, *a* for area. See the continuation for details.

2.Triples with common hypothenuse h.

If gcd(a,b)= 1, then any odd prime divisor of $h = a^2 + b^2$ is of the form $4m + 1$. See [4, Theorem 13].

Because h is odd, it is necessary that its prime factorization has the form

$$(2.1) \quad \begin{cases} h = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot_n^{\beta_n} \\ \text{with pairwise different primes } p_i \equiv 1 \pmod 4 \text{ and } \beta_i \geqq 1 \end{cases}$$

Due to Fermat, each prime p of the form $4m + 1$ can be written uniquely as a sum of two squares: $p = a^2 + b^2$, up to permutation of the squares. And we know from the remark at the beginning, that a, b have different parity.

Whenever it comes down to the question of discussing representations of a positive integer as a sum of two squares, we need to know two identities, which can be obtained by multiplying gaussian integers z, z' and using $|z| \cdot |z'| = |z \cdot z'|$:

$$(2.2) \qquad \begin{cases} (r+is)(u+iv) = (ru-sv) + i(rv+su) \\ (r-is)(u+iv) = (ru+sv) + i(rv-su) \end{cases}$$

which implies

$$(2.3) \qquad \begin{cases} (r^2+s^2)\cdot(u^2+v^2) = (ru-sv)^2 + (rv+su)^2 \\ (r^2+s^2)\cdot(u^2+v^2) = (ru+sv)^2 + (rv-su)^2 \end{cases}$$

Therefore, if we can represent factors as a sum of two squares, (2.3) gives us its product as sums of two squares. Converseley, any sum of two squares of a product can be decomposed.

More: Let us call a representation of a number as a sum of two squares $a^2 + b^2$ *proper*, if $gcd(a, b) = 1$. The unique proper representation for a prime power as well as the total of 2^{n-1} different proper representations of h can be generated by (2.3) with the knowlege of the representations of the primes p_i. Each additional prime power $p_i^{\beta_i}$ doubles the number of representations. Euler and Fermat have to be mentioned concerning these statements [16, Chap.II, §VIII and §IX]. The parity condition is respected by the two compositions (2.3).

Summarized, we have the following

THEOREM 1. *If $h > 1$ has the form (2.1), there exist exactly 2^{n-1} different primitive pythagorean triples with $h^2 = x^2 + y^2$, which can be generated by applying (2.3). If h is not of the form (2.1), there exist no primitive pythagorean triple.*

Examples: The smallest h with exactly

(a) 1 ppt is $5 = 2^2 + 1^2$ with the triple $[4, 3, 5]$

(b) 2 ppt is $5 \cdot 13 = 65 = (2^2+1^2)(3^2+2^2) = (6 \pm 2)^2 + (4 \mp 3)^2 = 8^2 + 1^2 = 4^2 + 7^2$ with triples $[16, 63, 65]$ $[56, 33, 65]$.

(c) 4 ppt is $65 \cdot 17 = 1105$. From $[8, 1], [7, 4]$ for 65 with the use of $[4, 1]$ for 17 we get:

$$[33,4] \longleftrightarrow [264,1073,1105] \qquad [31,12] \longleftrightarrow [744,817,1105]$$
$$[32,9] \longleftrightarrow [576,943,1105] \qquad [24,23] \longleftrightarrow [1104,47,1105]$$

(d) 128 ppt is $5 \cdot 13 \cdot 17 \cdot 29 \cdot 37 \cdot 41 \cdot 53 \cdot 61 = 138'863'452'745$

The first elements of the ordered sequence of h–values with

(1) 4 ppt are: 1105 1885 2405 2465 2665 3145 3445 3485 3965 4505 4745 5185 ...
Only the first two, marked with h, could be shown in Fig. 2.

(2) 8 ppt are: 32'045 40'885 45'305 58'565 67'405 69'745 77'285 80'665...

DISTRIBUTION OF TRIPLES WITH COMMON HYPOTHENUSE.

Asymtotic behavior of the number $\pi(x,m,r)$ of all primes $p \leqq x$ with $p \equiv r \pmod m$ and $gcd(r,m) = 1$, as $x \to \infty$, so called *primes in arithmetic progression*, (see [9, §4, Ch.III, Th.3.17]) :

$$\pi(x,m,r) \sim \frac{1}{\varphi(m)} \cdot \frac{x}{\log x} \tag{2.4}$$

The function φ is defined after (1.7) and log refers to the base $e \approx 2.718$.

In our case, with the notion $\pi(x)$ for the # of primes $\leqq x$, we get:

$$\pi(x,4,1) \sim \frac{1}{2} \cdot \frac{x}{\log x} = \frac{1}{2} \cdot \pi(x) \tag{2.5}$$

To generate h–values with several ppt, one has to deal with primes of the form $4m + 1$. With the computer, we got :

TABLE 1

Distribution of primes

x	# primes $\leqq x$	$\pi(x,4,1)$	$\frac{1}{2} \cdot \frac{\log x}{x - 1.08366}$
100	25	11	14
1'000	168	80	85.9
2'000	303	147	153.4
4'000	550	269	277.3
8'000	1007	499	506.1
16'000	1862	920	930.6
32'000	3432	1705	1722.3

By $H_n(x)$, we denote the # of $h \leqq x$ such that there exist exactly 2^{n-1} different ppt $[x,y,h]$ for each h. Calculations with the computer leads to Table 2 and Fig.4.

TABLE 2

Distribution of multiple ppt with common hypothenuse

x	$H_2(x)$: 2 triples	$H_3(x)$: 4 triples	$H_3(x)$: 8 triples
10'000	100	10	0
20'000	183	26	0
40'000	338	35	1
100'000	664	102	4
200'000	1'183	170	5
500'000	2'429	363	20
1'000'000	4'184	654	58
2'000'000	7'608	1'251	78
4'000'000	13'236	1'943	174
10'000'000	28'624	4'090	522
20'000'000	51'574	7'284	707
50'000'000	111'773	15'203	1'718
100'000'000	204'891	28'300	3'480
200'000'000	369'064	44'444	6'401
400'000'000	680'850	79'373	11'138
1'000'000'000	1'519'597	161'274	22'640
2'000'000'000	2'803'231	301'286	35'707

To discuss the ***asymtotic behaviour,*** we start with a classical result: For the number $\pi_n(x)$ of all positive integers $\leqq x$ of form (2.1), but *without* the condition $p_i \equiv 1 \pmod 4$, we have

$$\pi_n(x) \sim \frac{1}{(n-1)!} \cdot \frac{x \cdot (\log\log x)^{n-1}}{\log x} \qquad n = 1, 2, 3, \ldots \tag{2.6}$$

See [8, Ch.III, §4, Th.3.12] or [4, Sec.22.18, Th.437]. In the case $n = 1$, we get the prime number theory.

Using (2.6) and the probabilistic argument, that for each prime factor of the form $4m + 1$, we have to introduce a factor 2, it follows

$$H_n(x) \sim \frac{1}{2^n} \cdot \frac{1}{(n-1)!} \cdot \frac{x \cdot (\log\log x)^{n-1}}{\log x} \tag{2.7}$$

Furthermore

$$\frac{H_{n-1}(x)}{H_n(x)} \sim \frac{2(n-1)}{\log\log x} \qquad n = 2, 3, 4, \cdots \tag{2.8}$$

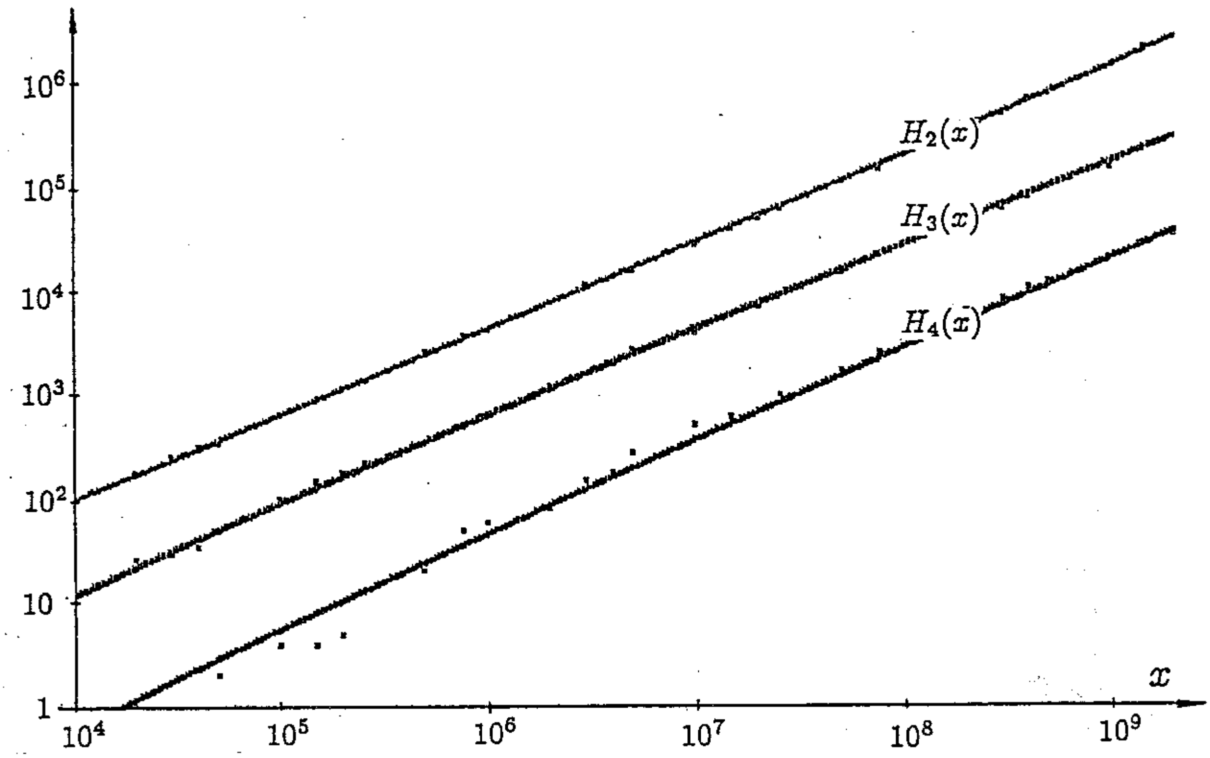

Fig. 4

and therefore

(2.9) $$\lim_{x\to\infty} \frac{H_{n-1}(x)}{H_n(x)} = 0$$

Therefore, asymtotically with respect to x, the # of hypothenuses $h \leqq x$, where h is associated to exactly 2^{n-1} different ppt, is arbitrarily small compared with those h with exactly 2^n different ppt. The asymtotic behaviour is completely different from what we have seen in Table 2 and Fig. 4. However, x has to be somehow "huge". The function $\log\log x$ *is extremely slowly increasing.*

Asymtotic behaviour of the # $H(x)$ of *all* ppt with $h \leqq x$:

$$H(x) = \sum_{n=1}^{\infty} 2^{n-1} \cdot H_n(x) \sim \frac{x}{2} \cdot \sum_{n=1}^{\infty} \frac{(\log\log x)^{n-1}}{(n-1)! \cdot \log x}$$

With the substitution $y = e^{e^x}$ we get

$$H(x) \sim \frac{x}{2} \cdot \sum_{n=1}^{\infty} \frac{y^{n-1}}{(n-1)! \cdot e^y} = \frac{x}{2}$$

However, the correct result in [7] is

(2.10) $$H(x) \sim \frac{x}{2\pi}$$

The above calculation is wrong, we cannot just sum up an infinity of asymptotical functions, as can be seen for :

$$f_n(x) = \begin{cases} 1 \text{ for } x \in (n, n+1) \\ 0 \text{ else} \end{cases} \tag{2.11}$$

Indeed, $\forall n, f_n(x) \sim 0$ as $x \to \infty$, but $\sum_{i=0}^{\infty} f_i = 1$. Nevertheless it is remarkable, that the result is correct up to the factor π.

FORMULA OF LEGENDRE. *For an arbitrarily given $h' = \gamma h > 0$, where h is of the form (2.1) and γ does not contain divisors of the form $4m+1$, the total # M of pythagorean triples with hypothenuse h' is given by*

$$2M + 1 = (2\beta_1 + 1) \cdot (2\beta_2 + 1) \cdots (2\beta_n + 1) \tag{2.12}$$

This is a straight forward result from Theorem 1. We count all possible ppt, whose hypothenuses are divisors d of h' .The ppt can than be multiplied by h'/d to get the desired triples:

For $n = 1$, we have β_1 triples : all possibilities are $d = {p_1}^k$ with $1 \leqq k \leqq \beta_1$.

For $n = 2$, we have $2\beta_1\beta_2 + \beta_1 + \beta_2$ triples, because $d = {p_1}^j {p_2}^k$ with $j, k \geqq 1$ has two common ppt.

By induction, we arrive at the general case.

SOME CONSEQUENCES.

(1) There exist a pythagorean triple iff the hypothenuse has at least one prime factor of the form $4m+1$. Example: The representation for $10 = 3^2 + 1$ is unique.
(2) All triples are not primitive iff $f > 1$.
(3) All triples associated with h are primitive iff h has the form (2.1) with $f = \beta_1 = \beta_2 = \cdots = 1$.
(4) For each given integer $k > 0$, there exist a h-value with exactly k different pythagorean triples. Example: The minimal value for h with three triples is 5^3. The triples are: $5^2 \cdot [4, 3, 5]$ $\quad 5 \cdot [24, 7, 5^2]$ $\quad [336, 527, 5^3]$.

3. Triples with common legsum s. From (1.2), for a given legsum we get

$$s = x + y = (a^2 - b^2) + 2ab = (a+b)^2 - 2b^2$$

With $u = a + b$ and v=b, this leads to Pells equation

$$u^2 - 2v^2 = s \qquad \text{with } gct(u, v) = 1 \text{ and } u = \text{ odd} \tag{3.1}$$

Because $a > b$, we have $a + b > 2b$ and

$$u > 2v > 0 \tag{3.2}$$

has to hold also.

Therefore, the solutions of (3.1) with the property (3.2) give the solutions of all ppt with legsum s, where $a = u - v, b = v$.

To deal with Pells equation, it makes sense to write

$$u^2 - 2v^2 = (u + v\sqrt{2})(u - v\sqrt{2}) \tag{3.3}$$

and to work in the *integer ring* $\mathbf{Z}[\sqrt{2}]$ consisting of elements $\alpha = u + v\sqrt{2}$ with *norm* $N(\alpha) = u^2 - v^2$. With the *conjugate element* $\alpha' = u - v\sqrt{2}$,we get

$$N(\alpha) = \alpha \cdot \alpha' = u^2 - 2v^2 \tag{3.4}$$

which is again (3.3). Indeed, solving Pells equation is the same as looking for elements with a given norm s.

Let us multiply the right hand side of

$$(r^2 - 2s^2)(u^2 - 2v^2) = (r + s\sqrt{2})(r - s\sqrt{2})(u + v\sqrt{2})(u - v\sqrt{2})$$

in two different ways:

(1) first and third, second and forth factor together.

(2) first and fourth, second and third factor together.

Then we get

$$\begin{cases} (r^2 - 2s^2)(u^2 - 2v^2) = (ru + 2sv)^2 - 2 \cdot (rv + su)^2 \\ (r^2 - 2s^2)(u^2 - 2v^2) = (ru - 2sv)^2 - 2 \cdot (rv - su)^2 \end{cases} \tag{3.5}$$

Elements with norm $+1$ or -1, so called *units*, play a particular role. The complete set of units in $\mathbf{Z}[\sqrt{2}]$ is the following: $\pm(3 + 2\sqrt{2})^m, m \in \mathbf{Z}$. If we knew one solution (u_0, v_0) of Pells equation, we were able to generate recursively an infinite set of solutions by introducing units of norm $+1$ in (3.5):

$$\begin{cases} u_{k+1} + v_{k+1}\sqrt{2} = (3 + 2\sqrt{2})(u_k + v\sqrt{2}) = (3u_k + 4v_k) + (+2u_k + 3v_k)\sqrt{2} \\ u_{k-1} + v_{k-1}\sqrt{2} = (3 - 2\sqrt{2})(u_k + v\sqrt{2}) = (3u_k - 4v_k) + (-2u_k + 3v_k)\sqrt{2} \end{cases} \tag{3.6}$$

$k = 0, 1, 2, \cdots$

Note that the indices in the first case are increasing and positive, in the second case decreasing and negative. Furthermore $(3 + 2\sqrt{2})^{-1} = (3 - 2\sqrt{2})$.

The generalized identities

$$(3.7)\qquad \begin{cases} (r^2+Rs^2)(u^2+Rv^2) = (ru-Rsv)^2 + R\cdot(rv+su)^2 \\ (r^2+Rs^2)(u^2+Rv^2) = (ru+Rsv)^2 + R\cdot(rv-su)^2 \end{cases}$$

contains the two special cases (2.3) and (3.5) by choosing $R = 1$ and $R = -2$ respectively. The introduced terminology holds also for the previous section,where we were in the ring $\mathbb{Z}[i]$ of the Gaussian integers with norm $N(u+iv) = |u+iv| = u^2+v^2$ and 4 units only, namely $\pm 1, \pm i$. The fact, that we have an infinity of units makes the legsum problem tougher than the hypothenuse problem. The relation "associated to" induces equivalence classes. Now we use results from the Gaussian Law of Quadratic Reciprocity and Quadratic Forms: See [8, Ch.VI,Th.111], [10, Ch.2], [1, Ch.4]:

LEMMA 1.
(A) There exist a solution of problem (3.1) iff all prime factors of s are of the form $8m \pm 1$.
(B) If $s > 1$ *is a product of n different prime powers, each prime of the form* $8m \pm 1$, *then there exist exactly* 2^{n-1} *different pairwise non-assiciated solutions of problem (3.1), therefore u and v are relatively prime.*
Note that 2^{n-1} *is* $\frac{1}{2}\cdot$ *# of solutions of the equation* $u^2 - 2 \equiv 0 \pmod{s}$.

Assuming s has the form mentioned in (B), the question is now: How many of the infinity of solutions of (3.1) fulfil the condition $u > 2v > 0$?

From

$$(3.8)\qquad \frac{u^2-4v^2}{u+2v} = \frac{2s-u^2}{u+2v} = u - 2v > 0$$

it follows that there exist only a *finite* number of such pairs (u,v), if any. Trivially, if (u, v) is a solution of (3.1), then all four combinations $(\pm u, \pm v)$ are solutions. More is said in

LEMMA 2. *Among the infinity* $(u,v) = (\pm u_k, \pm v_k)$ *of solutions of (3.1), where the set* $(u_k, v_k), k \in \mathbb{Z}$ *is associated to a fixed starting solution* (u_0, v_0) *described in (3.6), there exist exactly one which fulfils* $u > 2v > 0$.

Lemma 2 is already proved in [11], which is also interesting historically: It deals with "Problèmes de Fermat", in which Frenicle was involved. See also [16, Ch.II, §XII]. Here is a *new, shorter and from an algorithmic point of view constructive geometrical proof:*

With

$$(3.9)\qquad M = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \quad \text{and} \quad M^{-1} = \begin{pmatrix} 3 & -4 \\ -2 & 3 \end{pmatrix}$$

we describe (3.6) as a linear map of the plane in itself:

$$(3.10) \qquad \begin{pmatrix} u_{k+1} \\ v_{k+1} \end{pmatrix} = M \cdot \begin{pmatrix} u_k \\ v_k \end{pmatrix} \qquad \begin{pmatrix} u_{k-1} \\ v_{k-1} \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} u_k \\ v_k \end{pmatrix} \qquad k = 0, 1, 2, \cdots$$

Again: The indices in the first case are increasing and positive, in the second case decreasing and negative.

The eigenvectors of M and its inverse M^{-1} are

$$(3.11) \qquad \overrightarrow{f} = \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix} \quad \text{and} \quad \overrightarrow{g} = \begin{pmatrix} \sqrt{2} \\ -1 \end{pmatrix}$$

with eigenvalues $\lambda = 3 + 2\sqrt{2} \approx 5.83$ and $\mu = 3 - 2\sqrt{2} \approx 0.172$. For M, λ corresponds to $\overrightarrow{f}$ and μ to $\overrightarrow{g}$. For M^{-1}, λ corresponds to $\overrightarrow{g}$ and μ to $\overrightarrow{f}$.

We introduce a cartesian coordinate system for the integers u,v (see Fig. 5):

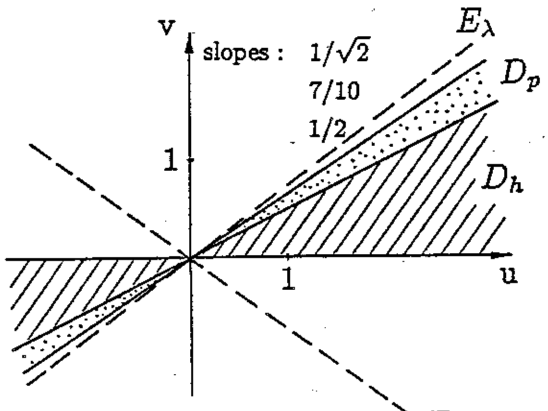

Fig. 5

There is at most one solution: Supposing there were two solutions

$$\overrightarrow{e}_i := \begin{pmatrix} u_i \\ v_i \end{pmatrix} \qquad \overrightarrow{e}_j := \begin{pmatrix} u_j \\ v_j \end{pmatrix} \qquad \text{with } i, j \in \mathbf{Z}, \quad i < j$$

This would imply $\overrightarrow{e_j} = M^k \cdot \overrightarrow{e_i}$ with $k = j - i > 0$.

Behavior of the linear map described by A: The two points associated with $\overrightarrow{e}_i$ and $\overrightarrow{e}_j$ have to lie within the hatched open domain D_h in Fig. 5.

Because

$$M \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 10 \\ 7 \end{pmatrix} \quad \text{and} \quad M \cdot \begin{pmatrix} 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

the image of D_h under the map M is the dotted open domain D_p, between the straight lines with slope $7/10$ and $1/2$ resp. D_p has obviously no point in common with D_h, beside the origin O, because the eigenvalue situation $\lambda > \mu > 0$ of A garantees that this image is closed enough to the eigenspace E_λ. The image of D_p will even be closer to E_λ etc. More: It is impossible, that one of the considered points could ly to the right and one to the left of O in D_h: The image of D_h with $u > 0$ is D_p with $u > 0$ and analogous with $u < 0$.

There exist a solution:
Using (A) of Lemma 1, there exist a pair $(u_m, v_m), m \in \mathbb{Z}$ among the set described in (3.6), independent of the given initial pair (u_0, v_0), such that either $u_m, v_m > 0$ or $u_m, v_m < 0$, because almost all points $A^k \cdot \vec{e}_0$ with $k > 0$ are "near" E_λ.

Similarly, almost all points $(A^{-1})^k \cdot \vec{e}_0$ are "near" E_μ. Supposing the first case, let us choose m now in such a way, that v_m is the *minimum* of all pairs with $v_m > 0$. We consider the linear combination

$$\vec{e_m} = \alpha \cdot \vec{f} + \beta \vec{g}$$

Because Pells equation holds, $u_m > \sqrt{2} \cdot v_m$ must be true and therefore, α and $\beta > 0$. This implies

$$\vec{e}_{m-k} = A^{-k} \cdot \vec{e}_m = \alpha \mu^k \cdot \vec{f} + \beta \lambda^k \cdot \vec{g} \qquad k = 0, 1, 2, \cdots$$

Because $0 < \mu < 1, \lambda > 1$, the scalars $\alpha\mu^k$ are strictely decreasing, $\beta\lambda^k$ strictly increasing. Obviously, the arguments of the vector sequence $\vec{e}_m, \vec{e}_{m-1}, \vec{e}_{m-2}, \cdots$ with reference to the abscissa in Fig. 5 is a strictely decreasing sequence, converging to $-\arctan(1/\sqrt{2})$. In particilar it follows from the minimum property for v_m, that $v_{m-1} < 0$. From $u_m = 3u_{m-1} + 4v^{m-1}, \quad v_m = 2u^{m-1} + 3v^{m-1}$ we get

$$u_m - 2v_m = -u_{m-1} - 2v_{m-1} = -(u_{m-1} - |v_{m-1}|)$$

Hence, either $u_m - 2v_m$ or $u_{m-1} - |v_{m-1}| > 0$. The case $u_m, v_m < 0$ can be treated similarily, choosing m such that v_m is the *maxima* among all pairs with $v_k < 0$ and exchanging the roles of M and M^{-1}.

Generating Primitive Pythagorean Triples with Common Legsum.
Using (3.5) for the n different prime powers of $s > 1$ gives 2^{n-1} solutions of (3.1), if all prime factors of s have the form $8m \pm 1$. Iteration in the sense of (3.6), stopping as soon as $|u| \geqq 2|v|$, generate the desired ppt with $a = |u| - |v|$ and $b = |v|$.

Examples: The smalles legsum with two different ppt is $s = 7 \cdot 17 = 119$. $u^2 - 2v^2 = 7$ has the solution $u = 3$, $v = 1$ and $u^2 - 2v^2 = 17$ has the solution $u = 5$, $v = 2$. Therefore using (3.5), $u^2 - 2v^2 = 119$ has the solutions $(u, v) = (19, 11)$ and $(11, 1)$. The first does not fulfil $u \geqq 2v$:

$$\begin{pmatrix} 3 & -4 \\ -2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 19 \\ 11 \end{pmatrix} = \begin{pmatrix} 13 \\ -5 \end{pmatrix}$$

One step is sufficient here. With (11,1) and (13,5), we get the following result: [10,1] generates [20,99,101] and [8,5] generates [80,39,89].

The smallest legsum with 4 different ppt is $s = 7 \cdot 17 \cdot 23 = 2737$. Using the two results for u, v above and the fact, that $u^2 - 2v^2 = 23$ has the solution (11,7), in each case after at most one step we get the generators: [37,36] [41,16] [43,12] [47,6] with the ppt [2664,73,2737] [1312,1425,2737] [1032,1705,2737] [564,2173,2737]. See also Fig. 2, where the particular points are marked with s if possible.
We have more parallels to the section dealing with common hypothenuses:

(1) Taking a legsum $s > 1$ of the right hand side form of (2.1), but with primes of the form $8m \pm 1$, Theorem 1 holds for s instead of h and the Legendre formula (2.12) as well.
(2) *Asymtotic behavior*: Using $\pi(x, 8, \pm 1)$ in (2.4), the probabilistic argument after (2.6) and the corresponding definition of $H_n(x)$ (see after Table 1), denoted by $S_n(x)$, obviously we get

$$(3.12) \qquad \frac{S_{n-1}}{S_n} \sim \frac{4(n-1)}{\log \log x} \qquad n = 2, 3, 4, \cdots$$

$$(3.13) \qquad \lim_{x \to \infty} \frac{S_{n-1}}{S_n} = 0$$

similar to (2.8) and (2.9).

4. Triples with Common Legdifference, Area, Perimeter, Inradius or Leg.

1. Common Legdifference d

With a common legdifference $d = |x - y|$ and (1.3) we have

$$(4.1) \quad d = |2ab - (a^2 - b^2)| = |2a^2 - (a-b)^2| \quad \text{with } a > b > 0, gct(a, b) = 1, a + b = \text{odd}$$

Also in this case, we have to deal with problem (3.1), however without the restrictive condition (3.2). So it is not astonishing to get an infinity of solutions, if all prime factors of d are of the form 8 ± 1 and no solution otherwise. In [18] we can find the easily verifiable statement:

If $[a, b]$ generates a ppt with legdifference d than also $[a + 2b, b]$.

Therefore, as soon as one knows one ppt, an infinity of ppt can be generated.

2. Common Area f

Searching for ppt with a common area f leads to the problem of finding f such that the equation

$$(4.2) \quad f = \frac{1}{2} \cdot xy = ab(a - b(a + b) \qquad \text{with} \quad a > b > 0, \quad gct(a, b) = 1, \quad a + b = \text{odd}$$

has several solutions. This seems to be a hard problem to solve. In [14] is mentioned:

The smallest area with a total of

(a) 2 ppt is $2 \cdot 3 \cdot 5 \cdot 7 = 210$, generated by [6,1] [5,2].

(b) 3 ppt is $210 \cdot 11 \cdot 13 \cdot 19 \cdot 23 = 13123110$, generated by [77,38] [78,55] [138,5].

An infinity of *pairs* of ppt with common area, but no information on more than 2 ppt with common area is given in [17]. Despite Eulers effort on this problem, not much more can be said today. Asymtotic behaviour for the # $A(x)$ of all ppt with area $\leqq x$ (see [7]) :

$$A(x) \sim c \cdot \sqrt{x} \qquad \text{with} \quad c = \frac{\Gamma(1/4)^2}{\sqrt{2} \cdot \pi^{5/2}} \approx 0.531340 \tag{4.3}$$

With $A_i(x)$, we denote the # of those areas $\leqq x$ which are associated with exactly i ppt. With the computer, we found for $x = 1'588'020$: $A_1 = 1976, A_2 = 22, A_3 = 1$ and $A_4 = A_5 = \cdots = 0$

In [5], an efficient criteria to generate rational right triangles whose areas are *rational* is given.

3. Common Perimeter p

$$p = x + y + h = 2ab + (a^2 - b^2) + (a^2 + b^2) = 2(a + b)a \tag{4.4}$$

with the conditions mentioned in (4.2).

Therefore $p =$ even is perimeter of a ppt iff

$$\frac{p}{2} = u \cdot v \quad \text{with} \quad u > v > 0 \quad \text{and} \quad gcd(u, v) = 1 \tag{4.5}$$

The generators are: $a = u - v, b = v$. $u > 2v$ and (4.5) imply:
# of isoperimetrical ppt with even perimeter $p =$ # of odd divisors u of p/2 with $\sqrt{\frac{p}{2}} < u < \sqrt{p}$ and $gcd(u, \frac{p}{2v}) = 1$.

Using Bertrands postulate, it is proven in [6], that for each $m > 0$, there exist a perimeter p with at least m isoperimetrical ppt.

In [2], a list of 5 perimeters between 14'280 and 103'740 is given ($60 \leqq a \leqq 210$), each one associated to 3 ppt. Asymptotic behaviour for the # $P(x)$ of all ppt with perimeter $\leqq x$ (see [7]) :

$$P(x) \sim \frac{\log 2}{\pi^2} \cdot x \tag{4.6}$$

4. Common Inradius i

$$i = \frac{2f}{p} = \frac{ab(a + b)(a - b)}{(a + b)a} = b(a - b) \qquad \text{with} \quad a - b > 0 \quad \text{and odd} \tag{4.7}$$

i is always an integer, and the situation is simpler than with the perimeter: If i has the prime factorization

$$(4.8)\qquad i = 2^{\beta} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n} \quad \text{with} \quad 2 < p_1 < p_2 < \cdots < p_n, \quad \beta \geqq 0, \quad \beta_i \geqq 1$$

we have

The number of ppt with common inradius $i = 2^n$

Because it is the # of ways to express i as a product of two relatively prime factors. An extensive study of this case can be found in [15, Sec.23.2].

5. Common Leg

This problem is left to the reader.

5.Triples with two common items.

THEOREM 3. *There exist no two non-congruent right triangles with one of the following items in common: hypothenuse, legsum, legdifference, area, perimeter, inradius, one leg.*

Note that the theorem is not restricted to integers.

Proof. Some of the $\binom{7}{2}$ possibilities are obvious, e.g. all with one common leg. In any case, the proof is of the kind as shown in the given representative examples.

(a) Common Hypothenuse h and Inradius i : Notations: f for the the area p for perimeter and α for the angle with $0 < \alpha < \pi/4$. With the abbreviations $s := \sin\alpha, c := \cos\beta$ we discuss the function

$$i(\alpha) = \frac{2f}{p} = \frac{2h^2 sc}{h + hs + hc}$$

with a fixed value h.

$$h \cdot \frac{di}{d\alpha} = \frac{d}{d\alpha} \frac{sc}{1+s+c} = \frac{c^2 + c^3 - s^2 - s^3}{(1+s+c)^2} = \frac{(c-s)(c^2 + cs + s^2 + c + s)}{(1+s+c)^2}$$

is clearly $> 0 \quad \forall \alpha \in (0, \pi/4)$.

(b) Common Legdifference $d = |x - y|$ and inradius i :

We consider $\delta := x - y$ to be fix:

$$i(x) = \frac{2x(x+\delta)}{2x + \delta + \sqrt{(x^2 + (x+\delta)^2}}$$

With $h = \sqrt{x^2 + (x+\delta)^2}$ and $D = 2x + \delta + h$ follows

$$D^2 \cdot \frac{di}{dx} = [2(x+\delta) + 2x][2x + \delta + h] - [2 + \frac{2x+\delta}{h}] \cdot 2x(x+\delta)$$

With $y = x + \delta$ we have

$$D^2 \cdot \frac{di}{dx} = (2x + 2y)(x + y + h) - (2 + \frac{x+y}{h}) \cdot 2xy = 2h^3 + 2(x+y)(h^2 - xy) > 0$$

because $h^2 - xy > 0$ for each rectangular triangle.

Acknowlegments. I would like to thank my students Rudolf Eicher and Ramon Furer for their computer work as well as their experimental approach into number theory. Both stimulated me for this work. Merci also to L.A. Szèkeley in Budapest for a private communication.

REFERENCES

[1] W.A. Adams and L.J. Goldstein, *Introduction to Number Theory*, Prentice—Hall, New Jersey, 1976.

[2] A. Anema, *Pythagorean Triangles with Equal Perimeters*, Scripta Mathematica, XV (1949), p. 89.

[3] L.E.Dickson, *History of the Theory of Numbers, Volume II*, University of Chicago Press, Chicago, 1931.

[4] G.H.Hardy and E.M.Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press, 1959.

[5] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, New York, Berlin, 1984.

[6] A.A. Krishnaswami, *On Isoperimetrical Pythagorean Triangles*, Tôhoku Math.J., 27 (1926), pp. 332–348.

[7] J. Lambek and L. Moser, *On the Distribution of Pythagorean Triangles*, Pacific J. Math., 5 (1955), pp. 73–83.

[8] T.Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York, 1964.

[9] W. Narkiewic, *Number Theory*, World Scientific, Singapore, 1977.

[10] I. Niven, *An Introduction to the Theory of Numbers*, Wiley, New York, 1980.

[11] P.Théophile Pepin, *Solution de quelques problèmes numériques*, Memoire della Pontificia Accademica dei Nuovi Lincei, volume settimo, 1891.

[12] H.Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, Basel, Progress in Mathematics, Vol.57, 1985.

[13] J.Rohlfs, *Mathematische Miniaturen 1, Lebendige Zahlen,Über die Summe von zwei Quadraten*, Birkhäuser,Boston, Basel, 1981.

[14] W. Sierpiński, *Pythagorean Triangles*, Yeshiva University, New York, 1962.

[15] B.M. Stewart, *Theory of Numbers*, Macmillan, New York, 1964.

[16] A.Weil, *Number Theory, An Approach through History*, Birkhäuser, Boston, Basel, 1983.

[17] W.P. Whitlock Jr., *Rational Right Triangles with Equal Area*, Scripta Mathematica, IX (1943), pp. 155–161.

[18] W.P. Whitlock Jr., *Pythagorean Triangles with a given Difference or Sum of Sides*, Scripta Mathematica, XI (1945), pp. 75–80.