A. BACKGROUND & PURPOSE – THE SEARCH FOR PYTHAGOREAN TRIPLES[1].

Three positive whole numbers $(\mathbf{a,b,c})$ which are such that $\mathbf{a}^2+\mathbf{b}^2=\mathbf{c}^2$ are called, collectively, a Pythagorean triple, and the three numbers **a**, **b**, and **c** represent the sides and hypotenuse of a right triangle.

Since this paper deals with Pythagorean triples and the right triangles associated with them, we shall use the abbreviation **PT** to stand for either a Pythagorean triple or the right triangle associated with it, depending upon the context.

As a youngster I knew that $(\mathbf{3,4,5})$ gave me a **PT**. I even knew that, by using similar triangles, other triples such as $(\mathbf{6,8,10})$ and $(\mathbf{15,20,25})$ also gave me **PT**s. Later on I learned that there were even other triples such as $(\mathbf{5,12,13})$ which were also **PT**s, and, moreover, which were essentially different from the $(\mathbf{3,4,5})$ **PT**.

Thus I saw that there were families of **PT**s with membership in a family based upon triangle similarity.

Moreover, it seemed that each family could be designated by a "reduced" triple. This led me to wonder about how many such families there were. I figured there were lots, but it didn't seem to matter much, because all the textbooks that I had in school and all the examples teachers ever put on the blackboard involving **PT**s always used something usually from the $(\mathbf{3,4,5})$ family or rarely from the $(\mathbf{5,12,13})$ family.

Someplace along the way I was told or perhaps I read that if r and s were positive integers with $r > s$, the triple $\left(r^2-s^2,\ 2rs,\ r^2+s^2\right)$ would always be a Pythagorean triple. The proof seemed a straight forward verification, so I believed it. But I think that it is worthwhile to perform this verification now[2], because it illustrates an interesting mathematical "lick," as they might call it in guitar playing.

Consider: $\left(r^2-s^2\right)^2+\left(2rs\right)^2=\left[r^4-2r^2s^2+s^4\right]+\left(4r^2s^2\right)=r^4+2r^2s^2+s^4=\left(r^2+s^2\right)^2$. And so you see that we do, indeed, have a **PT**.

So I finally understood that there were an infinite number of different families of Pythagorean triples, and, hence, an infinite number of essentially different right triangles.

But then, of course, came the question "Can all Pythagorean triples be generated by the method described above?" Teachers said "Yes," and I believed them. Now it's time to prove this.

B. PRELIMINARIES

1. PREFACE: There is nothing at all new in this paper; however, I did try to do most of the work without consulting outside references, and several of the arguments (as contorted as they may be) are my own. I

[1] In the references for this paper the Arabic numbers refer to footnotes and the Roman numerals refer to endnotes.
[2] I'll also be re-hashing this verification later in this paper.

credit the two "tricks" which you will find later in the paper to Chapter 2 of A Friendly Introduction to Number Theory by Joseph Silverman; however, I did try to give my own applications of those "tricks."

2. THE UNIVERSE: In the following discussion, let $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, 4, \ldots\}$ be the set of "natural numbers," i.e. the positive integers. This is our "Universe of Discourse."

3. NOTATION: "a | b" means "a divides b." In symbols: If $a, b \in \mathbb{N}$, then $a \mid b \overset{def}{\Leftrightarrow} \exists p \in \mathbb{N} \ni: \ b = ap$

In words:

1. a divides b if and only if there exists a number p in the set of positive integers such that b equals a times p. OR
2. a is a factor of b.

4. THEOREM (A): It's easy to prove that: $\boxed{m \mid n \Rightarrow m^2 \mid n^2}$

Here is a sketch of a proof:

Pf | $m \mid n \Rightarrow n = mp \quad (for\ some\ \ p \in \mathbb{N}) \ \Rightarrow n^2 = (mp)^2$

$\Rightarrow n^2 = m^2 p^2 \Rightarrow n^2 = m^2 q \ \ (where\ \ q = p^2 \in \mathbb{N}) \ \Rightarrow \ m^2 \mid n^2$

$\therefore \ \boxed{m \mid n \Rightarrow m^2 \mid n^2}$ •

5. REVIEW NOTE: $m \mid n \overset{is\ equivalent\ to}{\Leftrightarrow} n = mp \overset{is\ equivalent\ to}{\Leftrightarrow} \frac{n}{m} = p \in \mathbb{N}$

6. THEOREM [I](B): Also, we shall make use of the converse of Theorem A, namely,

If $m, n \in \mathbb{N}$, then $\boxed{m^2 \mid n^2 \Rightarrow m \mid n}$. That is "if m^2 divides n^2, then m divides n." Another way of saying this is that "if $n^2 = m^2 p \quad for\ some\ \ p \in \mathbb{N}$, then $n = mq \quad for\ some\ \ q \in \mathbb{N}$.

Here is one way to prove this: Suppose that $\frac{n}{m} \notin \mathbb{N}$ (this means that there are some factors of m which are not also factors of n), then $\left(\frac{n}{m}\right)^2 \notin \mathbb{N}$. Thus, $\frac{n^2}{m^2} \notin \mathbb{N}$. Thus, $\boxed{\frac{n}{m} \notin \mathbb{N} \Rightarrow \frac{n^2}{m^2} \notin \mathbb{N}.}$ •

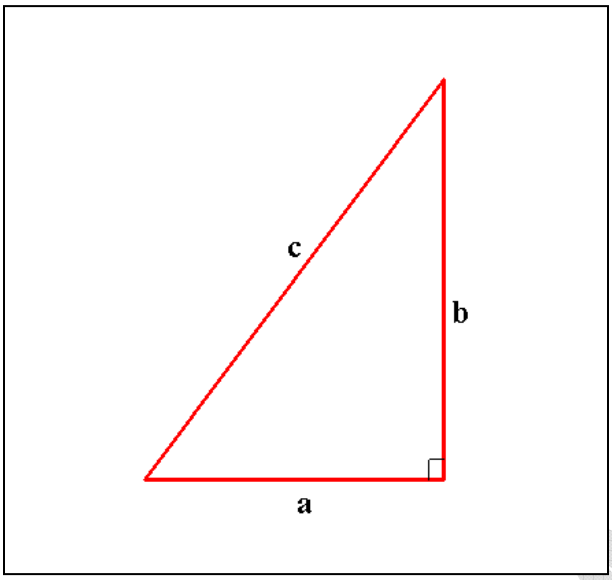
The contrapositive[3] of this implication is $\boxed{\frac{n^2}{m^2} \in \mathbb{N} \Rightarrow \frac{n}{m} \in \mathbb{N}.}$ •

Thus $m^2 \mid n^2 \Rightarrow \frac{n^2}{m^2} \in \mathbb{N} \Rightarrow \frac{n}{m} \in \mathbb{N} \Rightarrow m \mid n.$ Therefore, $\boxed{m^2 \mid n^2 \Rightarrow m \mid n}$ • .

[3] Recall: If $P \Rightarrow Q, \ then \ \sim Q \Rightarrow \sim P$ is the "contrapositive of the conditional." And thus, by double negation, if $\sim P \Rightarrow \sim Q, \ then \ Q \Rightarrow P.$ Also, we know that a conditional statement and its contrapositive are logically equivalent.

I'm sure that there are much better proofs of this little theorem, but this way was how I saw it.

C. RIGHT TRIANGLES and PYTHAGOREAN TRIPLES



1. INTRODUCTION: Here is a "typically-drawn" right triangle with the "usual lettering" – **a** and **b** are the arms and **c** is the hypotenuse. This labeling is not absolutely required; it is just more-or-less traditional. So I'll probably "stick to it." Thus, associated with each right triangle are the three numbers representing the lengths of the three sides.

Now we are investigating the cases where $\mathbf{a, b, c} \in \mathbb{N}$, that is where **a**, **b**, and **c** are whole numbers.

As we have stated earlier, in this case the triple $(\mathbf{a,b,c})$ is called a Pythagorean triple (**PT**) and **c** represents the length of the hypotenuse.

2. REDUCED PYTHAGOREAN TRIPLES: A fact (which is fairly obvious) is that any **PT** can be reduced by canceling out any and all factors common to **a**, **b**, and **c**. This cancelation reduces the **PT** and it also reduces the size of the associated right triangle to a smaller but similar[4] triangle.

Pf.|
If $(\mathbf{a,b,c}) \in \mathbf{P}_3$ and if $d = \gcd(\mathbf{a,b,c})$, then $\mathbf{a}^2 + \mathbf{b}^2 = \mathbf{c}^2$ *and* $\mathbf{a} = da,\ \mathbf{b} = db,\ \mathbf{c} = dc$. Thus we have $(da)^2 + (db)^2 = (dc)^2 \ \Rightarrow\ d^2a^2 + d^2b^2 = d^2c^2 \ \Rightarrow\ a^2 + b^2 = c^2$, so $(a,b,c) \in \mathbf{P}_3$ is the reduced form of $(\mathbf{a,b,c}) \in \mathbf{P}_3$. •

As a matter of convenience (to me), let's define $\mathbf{P}_3$ as the set of all Pythagorean triples. Thus, $\mathbf{P}_3 = \{(\mathbf{a,b,c}) \mid \mathbf{a,b,c} \in \mathbb{N},\ \mathbf{a}^2 + \mathbf{b}^2 = \mathbf{c}^2\}$. Now the idea of reducing a **PT** in $\mathbf{P}_3$ is a concept similar to that of reducing fractions within the set of rational numbers. It all goes back to the concept of "equivalence classes."

EXAMPLE: (3,4,5) is a well-known **PT**. It is the reduced form of (6,8,10), (9,12,15), (15,20,25), *etc.* all of which are elements of $\mathbf{P}_3$.

EXAMPLE: Conversely, (30,72,78) can be reduced to (15,36,39). This can be reduced further to (5,12,13), which is the reduced form. Each of these triples is an element of $\mathbf{P}_3$.

[4] "Similar" in the sense of Plane Geometry.

3. THE ODD-EVEN RULE:
As we shall see, in a reduced **PT** it is always the case that one of the arms is even and one is odd. We'll adopt the convention that **a** is <u>even</u> and **b** is <u>odd</u>. Now **a** may be greater than **b** or less than **b** – that is of no concern here. We'll simply take the position that **a** is even and **b** is odd.[5]

4. ANALYSIS OF $(\mathbf{a},\mathbf{b},\mathbf{c}) \in \mathbf{P}_3$ WITH RESPECT TO PARITY[6]:

Here is a short sequence of mini-theorems which help me understand the nature of Pythagorean triples.

1. If **a** and **b** are even, then **c** is even.

   <u>Pf</u>: **a** is even means $\mathbf{a} = 2i$ for some $i \in \mathbb{N}$ and **b** is even means $\mathbf{b} = 2j$ for some $j \in \mathbb{N}$. Thus,
   $$\mathbf{c}^2 = \mathbf{a}^2 + \mathbf{b}^2 = (2i)^2 + (2j)^2 = 4i^2 + 4j^2$$
   $$= 4\left(i^2 + j^2\right).$$

   So $4 \mid \mathbf{c}^2$ [since $\left(i^2 + j^2\right) \in \mathbb{N}$] and, thus, by Theorem (B) $2 \mid \mathbf{c}$. Consequently ***c*** is even. •

2. If **a** and **b** are even, then (**a,b,c**) is reducible. (This follows immediately from #1). •

3. If (**a,b,c**) is reduced, then **a** and **b** are not both even. (This is the contrapositive of #2). •

4. **a** and **b** cannot both be odd.

   <u>Pf</u>[7]**:** Suppose that **a** and **b** ***<u>are</u>*** both odd. Then $\mathbf{a} = 2m+1 \quad and \quad \mathbf{b} = 2n+1$. Thus
   $$\mathbf{c}^2 = \mathbf{a}^2 + \mathbf{b}^2 = (2m+1)^2 + (2n+1)^2$$
   $$= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 = 4\left(m^2 + m + n^2 + n\right) + 2$$
   $$= 4u + 2 \qquad (*)$$

   Now **c** has to be either odd or even.

---

[5] You may ask the question: Can **a** and **b** be equal? If **a**, **b**, and **c** are positive integers, then it follows that **a** and **b** cannot be equal, for suppose that they were equal. Then, say **b=a**, so $\mathbf{a}^2 + \mathbf{b}^2 = \mathbf{c}^2$ becomes $\mathbf{a}^2 + \mathbf{a}^2 = \mathbf{c}^2 \quad \therefore \quad 2\mathbf{a}^2 = \mathbf{c}^2 \quad \therefore \quad \mathbf{c} = \mathbf{a}\sqrt{2}$ and we conclude that **c** cannot be an integer. This contradicts our original assumption that **a**, **b**, and **c** were positive integers. Therefore, **a** cannot equal **b**.

[6] "Parity" means "oddness" or "evenness."

[7] This proof is a bit more complicated. I decided to offer a "proof by contradiction (and cases)."

So, Case 1: Suppose **c** is even:
But I conclude that **c** cannot be even, for if it were, then we would have $2 \mid \mathbf{c}$. But this implies $4 \mid \mathbf{c}^2$. However, by (*) above, $4 \nmid \mathbf{c}^2$. (See [8] below).

Case 2: Suppose **c** is odd:
But also, I conclude that **c** cannot be odd, for if it were, then we would have $\mathbf{c} = 2r+1 \quad and \quad \mathbf{c}^2 = 4r^2+4r+1 = 2\left(2r^2+2r\right)+1$. This means that $\mathbf{c}^2$ is odd, but by (*) above, $\mathbf{c}^2$ is even.

Thus it follows that there is no such **c** (Because there is no number in $\mathbb{N}$ which is neither odd nor even). Thus **a** and **b** cannot both be odd. •

5. In a reduced **PT**, a and **b** must be of opposite parity. (This follows from #2 & #3). •

6. If $(\mathbf{a},\mathbf{b},\mathbf{c}) \in \mathbf{P}_3$, then **a** and **b** are of opposite parity and **c** is odd. (And remember we are assuming in this paper that **a** is even and **b** is odd).

   Pf.| So let us suppose that **a** and **b** are of opposite parity with **a** even and **b** odd. Then $\mathbf{a} = 2p$ and $\mathbf{b} = 2q+1$ for some $p, q \in \mathbb{N}$. So
   $\mathbf{c}^2 = \mathbf{a}^2 + \mathbf{b}^2 = (2p)^2 + (2q+1)^2 = 4p^2+4q^2+4q+1 = 2\left(2p^2+2q^2+2q\right)+1.$
   Thus, we see that $\mathbf{c}^2$ is odd, and it follows that **c** is odd, because if **c** were even, $\mathbf{c}^2$ would be even. •

5. THE "r,s – GENERATOR" OF PT's: (Here we repeat, for the purpose of continuity of thought, the verification done at the beginning of this paper).
Suppose that $r, s \in \mathbb{N}$. Let us also suppose that $r > s$. And now consider the sum $\left(r^2-s^2\right)^2 + (2rs)^2$. We have

$$\left(r^2-s^2\right)^2 + (2rs)^2 = r^4 - 2r^2s^2 + s^4 + 4r^2s^2 = r^4 + 2r^2s^2 + s^4 = \left(r^2+s^2\right)^2.$$

Thus, summarizing: $\left(r^2-s^2\right)^2 + (2rs)^2 = \left(r^2+s^2\right)^2$.

And so it follows[9] that $\left(2rs,\ r^2-s^2,\ r^2+s^2\right) \in \mathbf{P}_3$

---

[8] By (*) we see that $\mathbf{c}^2$ has a remainder of 2 when divided by 4.

[9] It is pretty easy to see that $\left(2rs,\ r^2-s^2,\ r^2+s^2\right)$ is reduced iff r and s have no common factors.

Thus
$$r > s$$
$$a = 2rs$$
$$b = r^2 - s^2$$
$$c = r^2 + s^2 \qquad \textbf{scheme X}$$

generates Pythagorean triples.

6. THE CONVERSE ISSUE:

Here is the real reason for this paper:

My question now is "Are all **PT**'s generated by **scheme X** above?"

But I'm not going to try to directly answer that question. I think that it will be enough if I can show that for any reduced $(\mathbf{a,b,c}) \in \mathbf{P_3}$ there exists a relatively prime pair r,s such that $(\mathbf{a,b,c})$ is generated by r,s according to **scheme X**.

Here's where I got stuck for the longest time, and I finally had to peek.[II] The "trick" seems to come in two parts. The first part **[Trick #1]** is to consider a reduced **PT**, $(\mathbf{a,b,c})$ **,** and set

$$\mathbf{b}^2 = \mathbf{c}^2 - \mathbf{a}^2 = (\mathbf{c}+\mathbf{a})(\mathbf{c}-\mathbf{a}) \qquad (*)$$

Now what I need to convince you of is that **if** $(\mathbf{a,b,c}) \in \mathbf{P_3}$, **if c** and **a** have no common factors, and **if a** is even while **b** and **c** are odd, **then** $(\mathbf{c}+\mathbf{a})$ and $(\mathbf{c}-\mathbf{a})$ are both squares.

Here's how it works: If we look at the prime factors of $(\mathbf{c}+\mathbf{a})$ and of $(\mathbf{c}-\mathbf{a})$, we have $(\mathbf{c}+\mathbf{a}) = p_1 p_2 \cdots p_\alpha$ and $(\mathbf{c}-\mathbf{a}) = q_1 q_2 \cdots q_\beta$, where all the p's need not be different and all the q's need not be different, but none of the p's can equal any q and vice-versa. But in $\mathbf{b}^2$ the distinct prime factors must occur in multiples of two. Thus, $(\mathbf{c}+\mathbf{a})$ and $(\mathbf{c}-\mathbf{a})$ must both be squares.

Next we let
$$\rho^2 = \mathbf{c}+\mathbf{a}$$
$$\sigma^2 = \mathbf{c}-\mathbf{a}$$

and thus $2\mathbf{c} = \rho^2 + \sigma^2$ and $2\mathbf{a} = \rho^2 - \sigma^2$.

So what we've got here is $\boxed{\mathbf{c} = \dfrac{\rho^2+\sigma^2}{2} \quad \text{and} \quad \mathbf{a} = \dfrac{\rho^2-\sigma^2}{2}}$

This leads to $\mathbf{b}^2 = \mathbf{c}^2 - \mathbf{a}^2 = \left(\frac{\rho^2+\sigma^2}{2}\right)^2 - \left(\frac{\rho^2-\sigma^2}{2}\right)^2$

$$= \frac{1}{4}\left[\rho^4 + 2\rho^2\sigma^2 + \sigma^4 - \left(\rho^4 - 2\rho^2\sigma^2 + \sigma^4\right)\right]$$

$$= \frac{1}{4}\left(4\rho^2\sigma^2\right) = \rho^2\sigma^2$$

So $\boxed{\mathbf{b} = \rho\sigma}$

Consequently, our Pythagorean triple looks like this:

$$\boxed{(\mathbf{a},\mathbf{b},\mathbf{c}) = \left(\frac{\rho^2-\sigma^2}{2},\ \rho\sigma,\ \frac{\rho^2+\sigma^2}{2}\right)}$$

where **a** is even, **b** is odd, and **c** is the odd hypotenuse.

Now comes the second part of the "trick" [10] **[Trick #2]:** Let $r = \frac{\rho+\sigma}{2}$ *and* $s = \frac{\rho-\sigma}{2}$.

Then

- $rs = \frac{1}{4}\left(\rho^2 - \sigma^2\right) \Rightarrow 2rs = \frac{\rho^2-\sigma^2}{2}$, so $\boxed{\mathbf{a} = 2rs}$.
- $r^2 - s^2 = \left(\frac{\rho+\sigma}{2}\right)^2 - \left(\frac{\rho-\sigma}{2}\right)^2 = \frac{1}{4}\left[\rho^2 + 2\rho\sigma + \sigma^2 - \rho^2 + 2\rho\sigma - \sigma^2\right] = \rho\sigma$, so $\boxed{\mathbf{b} = r^2 - s^2}$.
- $r^2 + s^2 = \left(\frac{\rho+\sigma}{2}\right)^2 + \left(\frac{\rho-\sigma}{2}\right)^2 = \frac{1}{4}\left[\rho^2 + 2\rho\sigma + \sigma^2 + \rho^2 - 2\rho\sigma + \sigma^2\right] = \frac{1}{2}\left(\rho^2 + \sigma^2\right)$,

  so $\boxed{\mathbf{c} = r^2 + s^2}$.

Thus, any reduced **PT** can be expressed in the form

[10] This is a fairly standard transformation.

$\boxed{(\mathbf{a},\mathbf{b},\mathbf{c}) = \left(2rs,\ r^2 - s^2,\ r^2 + s^2\right)}$ •

And this is what I wanted to show!

7. INTERESTING SPIN-OFF

We now know that one side of a Pythagorean triple right triangle must be odd. So give me any odd number, and I can fairly quickly give you back a Pythagorean triple with that odd number as a side.[11]

Here's how it works. Let n be any odd number (odd positive integer). Then square it, subtract one, and divide the result by 2. This gives you the other side. Now add one to this and you've got the hypotenuse.

In other words, my claim is that $\left(n,\ \frac{n^2-1}{2},\ \frac{n^2-1}{2}+1\right) \in \mathbf{P}_3$ or, equivalently, $\left(n,\ \frac{n^2-1}{2},\ \frac{n^2+1}{2}\right) \in \mathbf{P}_3$.

Let's see if this is true!

$$n^2 + \left(\frac{n^2-1}{2}\right)^2 = n^2 + \frac{n^4-2n^2+1}{4} = \frac{4n^2+n^4-2n^2+1}{4} = \frac{n^4+2n^2+1}{4} = \left(\frac{n^2+1}{2}\right)^2.$$

So it is true.

8. TRIVIAL SPIN-OFF TO THE SPIN-OFF

Square any odd number and subtract one. The result is divisible by four.

==========++++++++++==========++++++++++==========++++++++++==========+++++++++

END NOTES

[I] I also have a much more complicated proof of Theorem(B): Prove $m^2 \mid n^2 \Rightarrow m \mid n$.

In the alternative, prove $n^2 = m^2 p \ \Rightarrow\ n = mq$.

Pf. | Suppose not, i.e. suppose that $n^2 = m^2 p \ \wedge\ n \neq mq$. Then $n = mq + r \quad with \quad 0 < r < m$.

Thus $n^2 = (mq + r)^2 = m^2 q^2 + 2mqr + r^2$

So, $m^2 p = m^2 q^2 + 2mqr + r^2$; thus, $m^2\left(q^2 - p\right) + 2mqr + r^2 = 0$. This is "quadratic in m." Therefore using the quadratic formula, we get

---

[11] There may be more than one such triangle.

$$m=\frac{-b\pm\sqrt{b^2-4ac}}{2a}=\frac{-2qr\pm\sqrt{\left(2qr\right)^2-4\left(q^2-p\right)r^2}}{2\left(q^2-p\right)}=\frac{-2qr\pm\sqrt{4q^2r^2-4q^2r^2+4pr^2}}{2\left(q^2-p\right)}$$

$$=\frac{-2qr\pm\sqrt{4pr^2}}{2\left(q^2-p\right)}=\frac{-2qr\pm 2r\sqrt{p}}{2\left(q^2-p\right)}=\frac{-qr\pm r\sqrt{p}}{q^2-p}$$

So $\boxed{m=\frac{-qr\pm r\sqrt{p}}{q^2-p}}$. Now this means that p must be a square, since q, r, and m are all integers. So we let $p=\rho^2$,

and thus we have $m=\frac{-qr\pm r\rho}{q^2-\rho^2}=\frac{-r\left(q\mp\rho\right)}{\left(q+\rho\right)\left(q-\rho\right)}$.

Consequently,

either $m=\frac{-r\left(q-\rho\right)}{\left(q+\rho\right)\left(q-\rho\right)}=\frac{-r}{q+\rho}$, which cannot be, as this number is negative, but m is positive,

or $m=\frac{-r\left(q+\rho\right)}{\left(q+\rho\right)\left(q-\rho\right)}=\frac{-r}{q-\rho}=\frac{r}{\rho-q}$,

which implies that $r=m\left(\rho-q\right)=m\rho-mq \;\Rightarrow\; mq+r=m\rho \;\Rightarrow\; n=m\rho \;\Rightarrow\; m\mid n.$

But this cannot be since the assumption was that $m\nmid n$.

Thus our assumption has led to a contradiction. Therefore $m\mid n$, and we have shown that $\boxed{m^2\mid n^2 \;\Rightarrow\; m\mid n}$ •

[II] In reference to the two tricks utilized above, see www.math.brown.edu/~jhs/frintch2ch3.pdf (referenced 20090104_sun). From A Friendly Introduction to Number Theory by Joseph H. Silverman Third Edition - ISBN: 0-13-186137-9 - © 2006 Pearson Prentice Hall - 439 pages