Continuing with the proof of Theorem 71.

Hence we have \(a^2 + b^2 + c^2 + d^2 = pk\), with \(p \equiv 3 \pmod{4}\) a prime, \(k\) odd and less than \(p - 1\). If \(k = 1\) there is nothing to prove.

Read this equation modulo \(k\). Writing \(a \equiv a_1 \pmod{k}\), \(b \equiv b_1 \pmod{k}\), \(c \equiv c_1 \pmod{k}\), \(d \equiv d_1 \pmod{k}\) (mod \(k\)), where \(|a_1|, |b_1|, |c_1|, |d_1| < \frac{k}{2}\). Hence \(a_1^2 + b_1^2 + c_1^2 + d_1^2 = kk_1\), where \(a_1^2 + b_1^2 + c_1^2 + d_1^2 < k^2\) and so \(k_1 < k\).

Hence we have

\[
\begin{align*}
& a^2 + b^2 + c^2 + d^2 = pk, \text{ with } k \text{ odd and } 1 < k < p, \\
& a_1^2 + b_1^2 + c_1^2 + d_1^2 = kk_1, \text{ with } 1 \leq k_1 < k.
\end{align*}
\]

and so

\[
\begin{align*}
pk^2k_1 &= (a^2 + b^2 + c^2 + d^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2) \\
&= (aa_1 + bb_1 + cc_1 + dd_1)^2 + \\
& (ab_1 - ba_1 + cd_1 - dc_1)^2 + \\
& (ac_1 - bd_1 - ca_1 + db_1)^2 + \\
& (ad_1 - bc_1 + cb_1 - da_1)^2.
\end{align*}
\]

Now

\[
\begin{align*}
aa_1 + bb_1 + cc_1 + dd_1 & \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{k} \\
ab_1 - ba_1 + cd_1 - dc_1 & \equiv a_1b_1 - b_1a_1 + c_1d_1 - d_1c_1 \equiv 0 \pmod{k} \\
ac_1 - bd_1 - ca_1 + db_1 & \equiv a_1c_1 - b_1d_1 - c_1a_1 + d_1b_1 \equiv 0 \pmod{k} \\
ad_1 - bc_1 + cb_1 - da_1 & \equiv a_1d_1 - b_1c_1 + c_1b_1 - d_1a_1 \equiv 0 \pmod{k}.
\end{align*}
\]

Hence if

\[
\begin{align*}
r &= aa_1 + bb_1 + cc_1 + dd_1 \\
s &= ab_1 - ba_1 + cd_1 - dc_1 \\
t &= ac_1 - bd_1 - ca_1 + db_1 \\
u &= ad_1 - bc_1 + cb_1 - da_1,
\end{align*}
\]

then \(k\) divides each of \(r, s, t, u\). Thus we have

\[
(a^2 + b^2 + c^2 + d^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2) = pk^2k_1 = r^2 + s^2 + t^2 + u^2,
\]

and so

\[
pk_1 = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2.
\]
Since $k_1 < k$, it follows that we began with a multiple $kp$ of $p$ written as a sum of four squares and we have now produced a smaller multiple $k_1p$ which is also a sum of four squares. This is the Method of Descent.

This process can be repeated until $k = 1$ and then we have written $p$ as a sum of four squares and completes the proof of Theorem 71.

To show this method in action, I want us to write the prime 13759 as a sum of 4 squares. First

$$0^2 + 1^2 + 283^2 + 457^2 = 21.13759.$$ 

The reader can check that this is correct.

The method requires that equation to be read modulo 21. We get

$$0^2 + 1^2 + 10^2 + (-5)^2 = 6.21.$$ 

Hence

$$0^2 + 1^2 + 283^2 + 457^2 = 21.13759$$

$$0^2 + 1^2 + 10^2 + (-5)^2 = 21.6.$$ 

Hence

$$13759.21^2.6 = (0^2 + 1^2 + 283^2 + 457^2)(0^2 + 1^2 + 10^2 + (-5)^2)$$

$$= (0.0 + 1.1 + 283.10 + 457(-5))^2 +$$

$$= (0.1 - 1.0 + 283(-5) - 457.10)^2 +$$

$$= (0.10 - 283.0 - 1.(-5) + 1.457)^2 +$$

$$= 546^2 + 5985^2 + 462^2 + 273^2$$ 

Now 21|546, 5985, 462 and also 273. Hence, dividing by 21², we have

$$13759.6 = 26^2 + 285^2 + 22^2 + 13^2.$$ 

We can write this as

$$13759.6 = 285^2 + 13^2 + 26^2 + 22^2,$$ and so

$$13759.3 = \left( \frac{285 + 13}{2} \right)^2 + \left( \frac{285 - 13}{2} \right)^2 + \left( \frac{26 + 22}{2} \right)^2 + \left( \frac{26 - 22}{2} \right)^2$$

$$= 149^2 + 136^2 + 24^2 + 2^2.$$ 

Repeating the descent, we have

$$13759.3 = 149^2 + 136^2 + 24^2 + 2^2$$

$$3 = (-1)^2 + 1^2 + 0^2 + (-1)^2.$$
Hence

\[ 13759.3^2 = (149^2 + 136^2 + 24^2 + 2^2)((-1)^2 + 1^2 + 0^2 + (-1)^2) \]
\[ = (149(-1) + 136.1 + 24.0 + 2(-1)^2) \]
\[ (149.1 - 136(-1) + 24(-1) - 2.0)^2 \]
\[ (149.0 - 136(-1) - 24(-1) + 2.1)^2 \]
\[ (149.(-1) + 136.0 - 24.1 - 2.(-1))^2 \]
\[ = 15^2 + 261^2 + 162^2 + 171^2. \]

Hence dividing by $3^2$, we have

\[ 13759 = 5^2 + 87^2 + 54^2 + 57^2. \]

Of course, there are more efficient ways to complete this result. I have slavishly applied the algorithm to let the reader see the Method of Descent in action. If on the other hand, we had noticed that

\[ 13759 = 0^2 + 1^2 + 457^2 + 283^2 \]
\[ 21 = 1^2 + 2^2 + 0^2 + 4^2, \]

then from 65, we would have

\[ 13759.21^2 = (0.1 + 1.2 + 457.0 + 283.4)^2 + \]
\[ (0.2 - 1.1 + 457.4 - 0.283)^2 + \]
\[ (0.0 - 1.4 - 457.1 + 283.2)^2 + \]
\[ (0.4 + 1.0 - 457.2 - 283.1)^2. \]

Hence

\[ 13759.21^2 = 1134^2 + 1827^2 + 105^2 + 1197^2, \text{ and so} \]
\[ 13759 = 54^2 + 87^2 + 5^2 + 57^2, \text{ the same result!} \]

This is a bit misleading because we could just as easily have had:

\[ 13759 = 0^2 + 1^2 + 457^2 + 283^2 \]
\[ 21 = 1^2 + 0^2 + 2^2 + 4^2, \]

and then from 65, we would have

\[ 13759.21^2 = (0.1 + 1.0 + 457.2 + 283.4)^2 \]
\[ + \ldots \]

This would not be helpful because 21 does not divide $0.1 + 1.0 + 457.2 + 283.4 = 2046$. So in general it is better to apply the method verbatim ... it always works!
COUNTABILITY ETC

Definition We say that a set $S$ is countable if it is finite or if it can be put in one to one correspondence with the natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$. A countably infinite set $S$ is said to have cardinality $\aleph_0$.

The following sets have cardinal $\aleph_0$:

1. $\mathbb{Z}$. We can set up a (1,1) correspondence between $\mathbb{Z}$ and $\mathbb{N}$ for example, $0 \rightarrow 1$, $1 \rightarrow 2$, $-1 \rightarrow 3$, $2 \rightarrow 4$, $-2 \rightarrow 5$, etc. We can even give a formula here. Define $\varphi(n) = 2n$, if $n > 0$ and $\varphi(n) = -2n + 1$ if $n < 0$. It is easy to see that $\varphi$ is a (1,1) correspondence.

2. $\mathbb{Z} \oplus \mathbb{Z}$. We can set up a (1,1) correspondence between $\mathbb{Z} \oplus \mathbb{Z}$ and $\mathbb{N}$ for example, $(0,0) \rightarrow 1$, $(0,1) \rightarrow 2, (-1,0) \rightarrow 3$, $(1,1) \rightarrow 4$, $(1,-1) \rightarrow 5$, $(-1,-1) \rightarrow 6$, etc. Geometrically first list all pairs $(a,b)$ of the same 'weight' $|a| + |b|$ in order. Then for all pairs of the same weight $k$ we count them in an anti-clockwise fashion around the origin. Clearly every pair $(a,b)$ is counted with some natural number and every natural number counts a unique pair. Thus we have a (1,1) correspondence, even if we don’t have a formula.

3. $\mathbb{Q}$. We set up a (1,1) correspondence as follows. List the finitely many rationals $x = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, $b > 0$ of weight $|a| + b$. Then count pairs in order of weight, just as we did with $\mathbb{Z} \oplus \mathbb{Z}$. 