MATH. SCAND. 52 (1983), 5–19

# SQUARES IN ARITHMETICAL PROGRESSIONS I

J. H. E. COHN

Fermat proved that it is impossible for four consecutive terms of an arithmetical progression all to be squares, if the common difference $d \neq 0$. Pocklington [1] proves this from his result that the equation $z^2 = x^4 - x^2y^2 + y^4$ has no solutions in integers with $xy(x^2-y^2) \neq 0$.

We shall exhibit a connection between the solubility in positive integers of the system

$$(1) \qquad a = \alpha^2; \quad a+2d = \beta^2; \quad a+nd = \gamma^2; \quad a+(n+2)d = \delta^2,$$

and the solutions in integers of

$$(2) \qquad z^2 = x^4 + (n^2-2)x^2y^2 + y^4 \quad \text{with } xy(x^2-y^2) \neq 0,$$

the case $n=1$ of which represents Pocklington's method. The cases $n=0$ and $n=2$ are clearly trivial for both systems of equations and we shall assume without further mention that $n \neq 0$ or 2. Specifically we prove

THEOREM 1. (i) *if* (2) *has any solutions at all, then it has infinitely many such with different ratios for* $x:y$;

(ii) (1) *has solutions if and only if* (2) *has*;

(iii) *if* (1) *has any solutions at all, then it has infinitely many with different ratios for* $a:d$.

PROOF. (i) If (2) has a solution then so has

$$(3) \qquad \{X^2 - n^2Y^2\}\cdot\{X^2-(n^2-4)Y^2\} = Z^2, \quad XYZ \neq 0,$$

namely $X=z$, $Y=xy$, $Z=|x^4-y^4|$, for we find with these values that

$$X^2-n^2Y^2 = z^2-n^2x^2y^2 = (x^2-y^2)^2 \quad \text{and}$$
$$X^2-(n^2-4)Y^2 = z^2-(n^2-4)x^2y^2 = (x^2+y^2)^2 .$$

Conversely, if (3) has a solution then so has (2), namely $\bar{x}=2XY$, $\bar{y}=Z$, $\bar{z}=|X^4(n^4-4n^2)Y^4|$. For with these values

Received March 2, 1981.

$$\begin{aligned}\bar{y}^2+(n^2-2)\bar{x}^2 &= \{X^2-n^2Y^2\}\{X^2-(n^2-4)Y^2\}+4(n^2-2)X^2Y^2\\ &= X^4+2(n^2-2)X^2Y^2+n^2(n^2-4)Y^4\\ &= \{X^2+n^2Y^2\}\cdot\{X^2+(n^2-4)Y^2\}\ .\end{aligned}$$

Thus

$$\begin{aligned}\bar{y}^4+(n^2-2)\bar{x}^2y^{-2}+\bar{x}^4 &= \{X^4-n^4Y^4\}\{X^4-(n^2-4)^2Y^4\}+16X^4Y^4\\ &= X^8-(2n^4-8n^2)X^4Y^4+n^4(n^2-4)^2Y^8\\ &= \{X^4-(n^4-4n^2)Y^4\}^2\\ &= \bar{z}^2\ .\end{aligned}$$

It remains to show that $\bar{x}^2 \neq \bar{y}^2$, but this must be so since otherwise we should obtain successively

$$\begin{aligned}Z^2 &= 4X^2Y^2\\ X^4-(2n^2-4)X^2Y^2+(n^4-4n^2)Y^4 &= 4X^2Y^2\\ (X^2-n^2Y^2)^2 &= (2nY^2)^2\\ X^2 &= (n^2\pm 2n)Y^2\\ (n\pm 1)^2 &= 1+\text{square}\ ,\end{aligned}$$

and this is not so if $n \neq 0$ or 2.

Now suppose that (2) has a solution and suppose without loss of generality that $x>y>0$ and that $(x,y)=1$. Then by the above reasoning we find a solution of (3) and from this a new solution of (2), $\bar{x}=2xyz$, $\bar{y}=x^4-y^4$, with an appropriate $\bar{z}$, the expression for which is rather complicated, and irrelevant for our purpose. Of course it will not necessarily follow that $\bar{x}>\bar{y}$ or that $(\bar{x},\bar{y})=1$, but at least $\bar{x}$ and $\bar{y}$ will be positive and unequal. Whether $\bar{x}$ or $\bar{y}$ is the greater is of no import, for we can interchange them if necessary. To obtain a new solution of (2) in which the variables $x$ and $y$ have no common factor we can now divide $\bar{x}$ and $\bar{y}$ by $(\bar{x},\bar{y})$ to obtain say $x^*$ and $y^*$ respectively. Now although $\bar{x}$ and $\bar{y}$ may have common factors, they have no factor in common with either $x$ or $y$, for if so, such a factor would share a prime factor with both $x$ and $y$ and this cannot occur by our initial assumption about $x$ and $y$. It follows therefore that $x^* \geqq xy$ and in fact $x^*y^*>xy$, with the sole possible exception being if $2z=x^4-y^4$. But this cannot occur for it would imply that $x$ and $y$ were both odd (since they cannot be both even) and hence that

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

But then $x^2-y^2$ would have to divide $nxy$ and if the quotient were $c$ we should find that $\{\frac{1}{2}(x^2+y^2)\}^2=1+c^2$ which is impossible as $c\neq 0$. It follows therefore that given any one initial solution with $(x,y)=1$ we can find another one with $(x^*,y^*)=1$ and $x^*y^*>xy$. We thus find in like fashion infinitely many such solutions no two of which can have the same ratio $x:y$.

(ii) If (1) has solutions, let $x=\alpha\beta$ and $y=\gamma\delta$. Then $x\neq y$ and

$$\begin{aligned} & x^4+(n^2-2)x^2y^2+y^4 \\ = \; & (a^2+2ad)^2+(n^2-2)(a^2+2ad)(a^2+(2n+2)ad+n(n+2)d^2)+ \\ & +(a^2+(2n+2)ad+n(n+2)d^2)^2 \\ = \; & (2nad+n(n+2)d^2)^2+n^2(a^2+2ad)(a^2+(2n+2)ad+n(n+2)d^2) \\ = \; & n^2\{a^4+(2n+4)a^3d+a^2d^2(4+n^2+2n+4n+4)+ \\ & +ad^3(4n+8+2n^2+4n)+(n+2)^2d^4\} \\ = \; & n^2\{a^2+(n+2)ad+(n+2)d^2\}^2\,, \end{aligned}$$

and so (2) has solutions.

If (2) has solutions, let $z^2=x^4+(n^2-2)x^2y^2+y^4$ and $(x,y)=1$ with $x>y>0$. Let $T=(x^2+y^2)z$ and $S=xy(x^2-y^2)>0$. Then

$$\begin{aligned} T^2-(n+2)^2S^2 \; &= \; \{x^4+(n^2-2)x^2y^2+y^4\}\{x^4+2x^2y^2+y^4\}- \\ & \quad -(n+2)^2x^2y^2(x^4-2x^2y^2+y^4) \\ &= \; x^8-(4n+4)x^6y^2+(4n^2+8n+6)x^4y^4-(4n+4)x^2y^6+y^8 \\ &= \; \{x^4-(2n+2)x^2y^2+y^4\}^2 \; = \; A^2, \quad \text{say}\,, \end{aligned}$$

and

$$T^2-(n-2)^2S^2 \; = \; \{x^4+(2n-2)x^2y^2+y^4\}^2 \; = \; B^2, \quad \text{say, similarly}\,.$$

Now $B=(x^2-y^2)^2+2nx^2y^2\neq 0$ and we shall show that $A$ does not vanish either. For if $A$ were zero then $(x^2-y^2)^2=2nx^2y^2$ and so $z^2=(x^2-y^2)^2+n^2x^2y^2=(n^2+2n)x^2y^2$ would imply that $n^2+2n$ were a perfect square, which is impossible as $n\neq 0$ or 2.

To complete the proof that (1) has solutions it would now suffice to be able to deduce from the above that $T\pm(n+2)S$ and $T\pm(n-2)S$ were all perfect squares and then write $a=T-(n+2)S$, $d=2S$. Unfortunately, the various common factors which can arise are troublesome and so we proceed as follows. Let

$$\tau \; = \; T^4-(n^2-4)^2S^4 \quad \text{and} \quad \sigma \; = \; 2ABST\neq 0\,.$$

Then

$$\begin{aligned}\tau &= T^2(T^2-(n+2)^2S^2)+(n+2)^2S^2(T^2-(n-2)^2S^2)\\ &= A^2T^2+(n+2)^2B^2S^2\,,\end{aligned}$$

and so

$$\tau \pm (n+2)\sigma = (AT \pm (n+2)BS)^2$$

and similarly

$$\tau \pm (n-2)\sigma = (BT \pm (n-2)AS)^2\,.$$

Now let $a=\tau-(n+2)\sigma$, $d=2\sigma \neq 0$. Then $a$, $a+2d$, $a+nd$, and $a+(n+2)d$ are all perfect squares, as required.

(iii) Given a solution of (1) we see that (2) has a solution and hence infinitely many such with different ratios for $x:y$. Hence we can apply the algorithm above to produce arithmetical progressions satisfying (1) and since there can only be finitely many distinct ratios $x:y$ which yield a given ratio $a:d$, the proof is complete.

As a result of the above, we now consider the system (2) in more detail. For any solution of (2) we define $W(x,y,z)=(x^2+y^2)z$, a positive integer, and so if there are solutions at all, there will be one or more that minimise $W$. Such a solution we shall call a minimal solution; it is clear that for a minimal solution $(x,y)=1$ and so at least one of $x$ and $y$ will be odd. We shall assume that $y$ is odd. If in addition $x$ is also odd, then we shall assume that $x>y$.

LEMMA 1. *For a minimal solution of* (2), *if* $m=(x^2-y^2,n)$ *then* $m \leqq (2n)^{\frac{1}{2}}$; *if in addition* $nxy/m$ *is odd then* $m \leqq (\frac{1}{2}n)^{\frac{1}{2}}$.

PROOF. For a minimal solution, $z^2=(x^2-y^2)^2+(nxy)^2$ and since $(x,y)=1$ it easily follows that $(x^2-y^2,nxy)=m$. Hence

$$\left\{\frac{z}{m}\right\}^2 = \left\{\frac{x^2-y^2}{m}\right\}^2+\left\{\frac{nxy}{m}\right\}^2,$$

where the two summands have no common factor. Hence one of them is odd and the other even.

CASE 1. *If* $nxy/m$ *is odd*. Then for some positive integers $\lambda,\mu$ of opposite parity

$$nxy = (\lambda^2-\mu^2)m$$
$$x^2-y^2 = 2\lambda\mu m$$
$$z = (\lambda^2+\mu^2)m$$

and so

$$\left\{\frac{n(x^2+y^2)}{2m}\right\}^2 = n^2\left\{\frac{x^2-y^2}{2m}\right\}^2+\left\{\frac{nxy}{m}\right\}^2$$
$$= n^2\lambda^2\mu^2+(\lambda^2-\mu^2)^2 ,$$

an equation of the same form as (2) but with a new value for $W$, $W_1$ given by

$$W_1 = (\lambda^2+\mu^2) . \quad \frac{n(x^2+y^2)}{2m}$$
$$= \frac{nz(x^2+y^2)}{2m^2}$$
$$= \frac{nW}{2m^2} ,$$

and descent applies unless $m \leqq (\frac{1}{2}n)^{\frac{1}{2}}$.

CASE 2. *If $nxy/m$ is even.* We then obtain in similar fashion

$$x^2-y^2 = (\lambda^2-\mu^2)m$$
$$nxy = 2\lambda\mu m$$
$$z = (\lambda^2+\mu^2)m ,$$

and so

$$\left\{\frac{n(x^2+y^2)}{m}\right\}^2 = n^2\left\{\frac{x^2-y^2}{m}\right\}^2+4\left\{\frac{nxy}{m}\right\}^2$$
$$= n^2(\lambda^2-\mu^2)^2+16\lambda^2\mu^2$$
$$= n^2X^2Y^2+(X^2-Y^2)^2 ,$$

where $X=\lambda+\mu$ and $Y=\lambda-\mu$. Again we have an equation of the same form (2) with a new $W$,

$$W_1 = (X^2+Y^2)\cdot\frac{n(x^2+y^2)}{m}$$
$$= 2(\lambda^2+\mu^2)\cdot\frac{n(x^2+y^2)}{m}$$

$$= \frac{2n}{m^2} W,$$

and descent applies unless $m \leqq (2n)^{\frac{1}{2}}$.

Throughout the following $m$ will denote $(x^2 - y^2, n)$.

LEMMA 2. *If* $2 \parallel n$ *and* $m$ *is odd then* $m \equiv \pm 1 \pmod 8$.

PROOF. We have $nxy/m$ is even, and so as above

$$x^2 - y^2 = (\lambda^2 - \mu^2)m$$

$$nxy = 2\lambda\mu m .$$

Since $2 \parallel n$ and $m$ is odd, $xy$ and $\lambda\mu$ are divisible by the same power of 2. If now $2 \parallel xy$, then each of $x^2 - y^2$ and $\lambda^2 - \mu^2$ is congruent to 3 or 5 (mod 8), whereas if $4 \mid xy$ both expressions are congruent to 1 or 7 (mod 8). In either case the statement of the lemma follows.

LEMMA 3. *If* $2 \parallel m$ *then* $n/m \equiv \pm 1 \pmod 8$.

PROOF. Since $m$ is even, $x$ must be odd and since $4 \nmid m$, $4 \nmid n$, since now $8 \mid (x^2 - y^2)$. Thus $nxy/m$ is odd, and so as in the proof of Lemma 1,

$$nxy = (\lambda^2 - \mu^2)m$$

$$x^2 - y^2 = 2\lambda\mu m .$$

Since $x$ and $y$ are both odd, we may define integers $e$ and $f$ of opposite parity by $e = \frac{1}{2}(x+y)$ and $f = \frac{1}{2}(x-y)$ obtaining

$$n(e^2 - f^2) = (\lambda^2 - \mu^2)m$$

$$ef = (\tfrac{1}{2}m)\lambda\mu ,$$

and the conclusion now follows as in the proof of the preceding lemma.

LEMMA 4. *For any solution of* (2) $x^2 + y^2 > 2n^{\frac{1}{2}}$.

PROOF. We have

$$z^2 = (nxy)^2 + (x^2 - y^2)^2 > (nxy)^2 ,$$

and so $z \geqq nxy + 1$. Thus

$$(x^2 + y^2)^2 > (x^2 - y^2)^2$$

$$\begin{aligned}
&= z^2-(nxy)^2 \\
&\geqq (nxy+1)^2-(nxy)^2 \\
&= 2nxy+1 \\
&> 4n, \qquad \text{since } xy(x^2-y^2) \neq 0 .
\end{aligned}$$

LEMMA 5. *Suppose that $n$ is odd, and that* (2) *has solutions. Then there exist positive integers $a$, $b$, $c$, $d$, $r$, $s$, $t$, $\lambda$, and $\mu$ with $c$ and $d$ both odd, $a$, $b$, $c$, and $d$ coprime in pairs, with $t=1$ or 2 such that $y=cd$, $x=tab$ is a minimal solution of* (2) *which defines $m$ such that $\lambda\mu=n/m$, $rs=n^2-4$ and*

$$\begin{aligned}
rc^2-m\mu^2d^2 &= 2ta^2 \\
m\lambda^2c^2-sd^2 &= 2tb^2, \qquad \textit{where}
\end{aligned}$$

(a) *if $t=1$, $a$ and $b$ are both odd and $\lambda<\mu$;*
(b) *if $t=2$, $r$ and $m$ cannot both be squares, and $b^2-a^2\equiv m \pmod 4$.*

PROOF. Let $x,y$ provide a minimal solution with $y$ odd. Then

$$\begin{aligned}
4z^2 &= 4x^4+4(n^2-2)x^2y^2+4y^4 \\
&= \{2(x^2-y^2)+n^2y^2\}^2-n^2(n^2-4)y^4
\end{aligned}$$

and so

$$(n^2-4)n^2y^4 = \{2(x^2-y^2)+n^2y^2+2z\}\cdot\{2(x^2-y^2)+n^2y^2-2z\} .$$

Now $m=(x^2-y^2,n)$ divides $z$ and so both factors on the right. Thus

$$\begin{aligned}
(n^2-4)\left(\frac{n}{m}\right)^2y^4 &= \left\{\frac{2(x^2-y^2)}{m}+\frac{n^2y^2}{m}+\frac{2z}{m}\right\}\cdot\left\{\frac{2(x^2-y^2)}{m}+\frac{n^2y^2}{m}-\frac{2z}{m}\right\} \\
&= A\cdot B, \qquad \text{say} .
\end{aligned}$$

Now the left hand side of this equation is odd, since $n$ and $y$ are odd, and hence $A$ and $B$ are both odd. Let $p$ denote any prime dividing $(A,B)$. Then $p$ is odd, and divides both $AB$ and $\frac{1}{2}(A+B)$, i.e. both

$$(n^2-4)\left(\frac{n}{m}\right)^2y^4 \quad \text{and} \quad \frac{2(x^2-y^2)}{m}+\frac{n^2y^2}{m} .$$

In the first place we observe that $p$ cannot divide $y$, otherwise it would also have to divide $x$, impossible since $x$ and $y$ were supposed to provide a minimal solution. Similarly $p$ cannot divide $n/m$ otherwise it would also have to divide $(x^2-y^2)/m$, contradicting the definition of $m$. Hence $p$ can only divide $n^2-4$, and then it would also divide $x^2+y^2$, and must necessarily be congruent to 1 modulo 4. Hence we obtain for suitable $c$, $d$, $r$, $s$, $\lambda$, and $\mu$, $A=r\lambda^2c^4$, $B=s\mu^2d^4$, where $y=cd$ is odd; $rs=n^2-4$; $\lambda\mu=n/m$ and $(A,B)=(r,s)$ which has only prime factors congruent to 1 modulo 4. Then adding $A$ and $B$ to eliminate $z$ gives

$$r\lambda^2c^4+s\mu^2d^4 = 4(x^2-y^2)m^{-1}+2n^2y^2m^{-1}$$

and so solving for $x^2$ and substituting $y=cd$ yields

$$\begin{aligned}4x^2 &= rm\lambda^2c^4-(2n^2-4)c^2d^2+sm\mu^2d^4\\ &= (rc^2-m\mu^2d^2)\cdot(m\lambda^2c^2-sd^2)\\ &= C\cdot D, \quad \text{say}.\end{aligned}$$

Now both $C$ and $D$ are even since $r$, $s$, $c$, $d$, $\lambda$, $\mu$, and $m$ are all odd, and so $2\mid(C,D)$. However we find that

$$m\mu^2D-sC = (n^2-rs)c^2 = 4c^2; \qquad rD-m\lambda^2C = 4d^2,$$

and so since $c$ and $d$ are coprime, $(C,D)$ divides 4. Hence we obtain $C=\pm2ta^2$, $D=\pm2tb^2$ and $x=tab$, where $t=1$ or 2. Apart from the $\pm$ sign these are the required equations. But the $\pm$ sign can be removed by interchanging in pairs $c$ and $d$; $\lambda$ and $\mu$; $a$ and $b$ if necessary. Here $(a,b)=1$ and since $x=2tab$, $y=cd$, it then follows that $a$, $b$, $c$, and $d$ are pairwise coprime.

If $t=1$, $a$ cannot be even for if it were we should find that $r\equiv m \pmod 4$ and so since $rs=n^2-4\equiv1 \pmod 4$ we should find that $s\equiv m \pmod 4$ and so $2b^2\equiv0 \pmod 4$ would force $b$ to be even also, which is impossible. Similarly $b$ must be odd. Finally, in this case we may assume that $\lambda<\mu$. For certainly $\lambda\neq\mu$ since $(\lambda,\mu)=1$ and $m<n$ by Lemma 1, and if $\lambda>\mu$ then we find that $rb^2-m\lambda^2a^2=2d^2$, $m\mu^2b^2-sa^2=2c^2$, and now $\mu<\lambda$, and so the result follows on interchanging $c$ and $b$; $d$ and $a$; $x$ and $y$ in pairs. This concludes the first case.

If $t=2$, then we obtain $rb^2-m\lambda^2a^2=d^2$, $m\mu^2b^2-sa^2=c^2$. Since $r$, $c$, and $m$ are all odd, $r\equiv m \pmod 4$ and so $a$ and $b$ have opposite parity. If $m\equiv1 \pmod 4$, then $a$ must be even and $b$ odd, whereas if $m\equiv3 \pmod 4$, then the reverse holds; in either case $b^2-a^2\equiv m \pmod 4$. Finally, we must show that $r$ and $m$ cannot both be perfect squares if $t=2$. We observe first that $4z/m=A-B=r\lambda^2c^4-s\mu^2d^4$ and so

$$\begin{aligned}4z &= rc^2(sd^2+4b^2)-sd^2(rc^2-4a^2)\\ z &= rb^2c^2+sa^2d^2 > rbc.\end{aligned}$$

Now suppose if possible that $r=R^2$ and $m=M^2$. Then the first equation becomes $(Rc)^2=(M\mu d)^2+(2a)^2$ where no prime divides both $Rc$ and $M\mu d$. For suppose on the contrary that a prime $p$ did divide them both. Then $p \neq 2$, since $Rc$ is odd, and thus we should have that $p \mid a$. But then $p \nmid cd$. Thus $p \mid R$ and $p \mid M\mu$. But $M\mu$ divides $n$ and $n$ and $R$ have no common factor, since $R$ divides $n^2-4$ and is odd. Thus we must have for some suitable integers $e$ and $f$ with no common factor,

$$\begin{aligned} Rc &= e^2+f^2 \\ a &= ef \\ M\mu d &= e^2-f^2 . \end{aligned}$$

Then

$$\begin{aligned} (2bM R\mu)^2 &= M^4\lambda^2\mu^2(Rc)^2 - R^2s(M \mu d)^2 \\ &= n^2(e^2+f^2)^2-(n^2-4)(e^2-f^2)^2 \end{aligned}$$

and so

$$(bMR\mu)^2 = e^4+(n^2-2)e^2f^2+f^4 ,$$

and equation of the same form as (2). But now the new $W, W_1$ satisfies

$$\begin{aligned} W_1 &= bMR\mu(e^2+f^2) \\ &= bMR^2\mu c \\ &= M\mu rbc < M\mu z , \end{aligned}$$

and so this case is impossible by descent, unless $x^2+y^2<M\mu$.

To deal with the possibility that $x^2+y^2<M\mu$, we can as before rewrite our equations in the form

$$\begin{aligned} R^2b^2-M^2\lambda^2a^2 &= d^2 \\ M^2\mu^2b^2-sa^2 &= c^2 , \end{aligned}$$

and obtain just as before, successively

$$\begin{aligned} Rb &= g^2+h^2 \\ M\lambda a &= 2gh \\ d &= g^2-h^2 , \\ (M\lambda Rc)^2 &= M^4\lambda^2\mu^2(g^2+h^2)^2-4rsg^2h^2 . \end{aligned}$$

Now let $G=g+h$, $H=g-h$. Then

$$\begin{aligned} (M\lambda Rc)^2 &= \tfrac{1}{4}n^2(G^2+H^2)^2-\tfrac{1}{4}(n^2-4)(G^2-H^2)^2 \\ &= G^4+(n^2-2)G^2H^2+H^4 , \end{aligned}$$

where now

$$\begin{aligned} W_2 &= M\lambda Rc(G^2+H^2) \\ &= 2M\lambda Rc(g^2+h^2) \\ &= 2M\lambda rbc \\ &< 2M\lambda z\,, \end{aligned}$$

and again descent applies unless $x^2+y^2<2M\lambda$.

But the conditions $x^2+y^2<M\mu$ and $x^2+y^2<2M\lambda$ cannot hold simultaneously, for together they would imply $(x^2+y^2)^2<2M^2\lambda\mu=2m\lambda\mu=2n$, impossible by Lemma 4.

This concludes the proof.

We next state without proof three more results which together deal with the various cases in which $n$ is even. In all cases the proofs are similar to the above, the differences concerning only the powers of 2 which arise.

LEMMA 6. *If there exists a solution of* (2) *which is minimal and has $n/m$ even, then there exists such a solution and positive integers $a$, $b$, $c$, $d$, $r$, $s$, $\lambda$ and $\mu$ with $c$ and $d$ both odd; $a$, $b$, $c$ and $d$ coprime in pairs; $(\lambda,\mu)=1$ and with $(r,s)$ divisible only by primes congruent to* 1 *modulo* 4; $rs=\frac{1}{4}n^2-1$; $\lambda\mu=n/(2m)$; $x=ab$; $y=cd$ *and with*

$$\begin{aligned} rc^2-m\mu^2d^2 &= a^2 \\ m\lambda^2c^2-sd^2 &= b^2\,, \end{aligned}$$

*where if $m$ is even, $a$ and $b$ are both odd and $\lambda<\mu$, and if $m$ is odd $b^2-a^2\equiv m$* (mod 4). *Also $r$ and $m$ cannot both be squares.*

LEMMA 7. *If there exists a minimal solution of* (2) *with $n/m$ odd and $4\mid n$, then there exists such a solution and odd positive integers $a$, $b$, $c$, $d$, $r$, $s$, $\lambda$ and $\mu$ with $a$, $b$, $c$, $d$ coprime in pairs; $(\lambda,\mu)=1$; $\lambda<\mu$; $(r,s)$ divisible only by primes congruent to* 1 *modulo* 4; $rs=\frac{1}{4}n^2-1$; $\lambda\mu=n/m$; $x=ab$; $y=cd$ *and with*

$$\begin{aligned} rc^2-\tfrac{1}{2}m\mu^2d^2 &= a^2 \\ \tfrac{1}{2}m\lambda^2c^2-sd^2 &= b^2 \end{aligned}$$

*and with $r$ and $\frac{1}{2}m$ not both squares.*

LEMMA 8. *If there exists a solution of* (2) *with $n/m$ odd and $2\,\|\,n$, then there exists such a solution and positive integers $a$, $b$, $c$, $d$, $r$, $s$, $\lambda$ and $\mu$ with $a$, $b$, $c$, $d$*

*coprime in pairs and all odd*; $(\lambda, \mu)=1$; $\lambda<\mu$; $(r,s)$ *divisible only by primes congruent to* 1 *modulo* 4; $\lambda\mu=n/m$; $rs=\frac{1}{16}(n^2-4)$; $x=ab$; $y=cd$ *and with*

$$2rc^2-\tfrac{1}{2}m\mu^2d^2 = a^2$$

$$\tfrac{1}{2}m\lambda^2c^2-2sd^2 = b^2 .$$

The above results can be used for many values of $n$ either to find solutions, where they exist, or to prove the non-existence of solutions. In order to aid the latter, we make the following

DEFINITION. *For* $i=1$, 3, 5 *and* 7, *let* $\varrho(i)$ *denote the number of distinct prime factors of* $(n^2-4)$, *and* $R(i)$ *the total number of prime factors, counting multiplicity, which are congruent to* $i$ *modulo* 8.

LEMMA 9. *If* $n$ *is odd, the case* $m=1$ *can only arise if there exist integers* $r, s$ *with* $rs=n^2-4$, $(r,s)$ *divisible only by primes congruent to* 1 *modulo* 4 *and*

*either* (a) $r\equiv 1 \pmod 8$; *$r$ not a square*; *$r$ divisible only by primes congruent to* 1 *modulo* 4 *and* $(r\mid P)=1$ *for every prime* $P$ *dividing* $n$,

*or* (b) $r\equiv 3 \pmod 8$; *every factor of $r$ congruent to* 1 *or* 3 *modulo* 8; *every factor of $s$ congruent to* 1 *or* 7 *modulo* 8 *and* $(2r\mid P)=1$ *for every prime* $P$ *dividing* $n$.

*In particular we must have* $\varrho(1)\geqq 1$ *or* $\varrho(5)\geqq 2$ *or* $\{\varrho(5)=0$ *and* $R(3)$ *odd*$\}$.

PROOF. Lemma 5 applies and so $rs=n^2-4$ with $(r,s)$ divisible only by primes congruent to 1 modulo 4, $\lambda\mu=n$ and

$$rc^2-\mu^2d^2 = 2ta^2$$

$$\lambda^2c^2-sd^2 = 2tb^2 .$$

If $t=1$, then $a$ and $b$ are both odd and so $r\equiv 3 \pmod 8$ and every factor of $r$ must be congruent to 1 or 3 modulo 8, every factor of $s$ must be congruent to 1 or 7 modulo 8. Now if $P\mid n$, then $P$ divides $\lambda$ or $\mu$. In the former case $(-2s\mid P)=1$, and since $rs\equiv -4 \pmod P$ $(2r\mid P)=1$; in the latter case $(2r\mid P)=1$ also.

If $t=2$, then $r\equiv 1 \pmod 8$, $r$ cannot be a square, every factor of $r\equiv 1 \pmod 4$ and $(r\mid P)=1$ as above.

Finally, we see that in case (a), $r$ must have either a prime factor congruent to 1 modulo 8, or else two distinct prime factors congruent to 5 modulo 8. In case (b) there can be no prime factors of $n^2-4$ congruent to 5 modulo 8 at all whereas all prime factors congruent to 3 modulo 8 divide $r$, and so $\varrho(5)=0$ and $R(3)$ must be odd.

In exactly the same way we may prove the following results whose proofs are omitted.

LEMMA 10. *If* $2 \parallel n$, *the case* $m=1$ *can only arise if there exists an integer* $r$ *dividing* $\frac{1}{4}n^2-1$, *with* $r$ *not a square, every factor of* $r$ *congruent to* 1 *modulo* 4 *and* $(r \mid P)=1$ *for every odd prime* $P$ *dividing* $n$. *In particular* $\varrho(1)+\varrho(5)\geqq 1$.

LEMMA 11. *If* $4 \mid n$, *the case* $m=1$ *can only occur if there exists an integer* $r$ *dividing* $\frac{1}{4}n^2-1$ *with* $r$ *not a square, every factor of* $r$ *congruent to* 1 *modulo* 4, $r \equiv 1 \pmod 8$ *and* $(r \mid P)=1$ *for every odd prime* $P$ *dividing* $n$. *In particular* $\varrho(1)\geqq 1$ *or* $\varrho(5)\geqq 2$.

THEOREM 2. *If* $n$ *is an odd prime, then a necessary condition for* (2) *to have solutions is that either* $\varrho(1)\geqq 1$ *or* $\varrho(5)\geqq 2$, *or* $\{\varrho(5)=0$ *and* $R(3)$ *is odd*$\}$.

PROOF. By Lemma 1, for any minimal solution $m\leqq(2n)^{\frac{1}{2}}$ and so $m=1$. The result then follows by Lemma 9.

THEOREM 3. *If* $n=2p$, *where* $p$ *denotes a prime*, $p=2$ *or* $p\equiv \pm 3 \pmod 8$, *then a necessary condition for* (2) *to have solutions is that* $\varrho(1)+\varrho(5)\geqq 1$.

PROOF. For $p=2$, the result was proved by Pocklington [1]. Suppose then that $p\equiv \pm 3 \pmod 8$. Then by Lemma 1, for a minimal solution $m\leqq(4p)^{\frac{1}{2}}<p$ if $p>4$. Thus $m=1$ or 2 if $p>4$, and $m=1, 2$ or 3 if $p=3$. By Lemma 2, the case $p=m=3$ cannot arise. By Lemma 3, the case $m=2$ does not arise. Thus $m=1$, and the result follows by Lemma 10.

THEOREM 4. *If* $n=4p$, *where* $p$ *denotes a prime, then a necessary condition for* (2) *to have solutions is that* $4p^2-1$ *have a factorisation* $rs$ *with* $(r \mid p)=1$ *if* $p$ *is odd, and with*

*either* (a) $r\equiv 1 \pmod 8$, *every factor of* $r$ *congruent to* 1 *modulo* 4, $r$ *not a square*,

*or* (b) $r\equiv 3 \pmod 8$; *every factor of* $r$ *congruent to* 1 *or* 3 *modulo* 8; *every factor of* $s$ *congruent to* 1 *or* 7 *modulo* 8.

*In particular* $\varrho(1)\geqq 1$ *or* $\varrho(5)\geqq 2$ *or* $\{\varrho(5)=0$ *and* $R(3)$ *is odd*$\}$.

PROOF. For a minimal solution we have by Lemma 1 that $m\leqq(8p)^{\frac{1}{2}}<p$ if $p>8$, and for these cases $m=1, 2$ or 4. The same holds if $p=2$. For $p=3$, we have the additional case $m=3$, whereas for $p=5$ or 7 the conditions given are satisfied and so the theorem is vacuously true. The cases $m=2$ for all $p$, and $m$

$=4$ for $p=2$ cannot arise, for $m$ divides $x^2-y^2$ and this latter expression if even at all requires both $x$ and $y$ to be odd, and then is divisible by 8.

For $m=1$, the result holds by Lemma 11. Suppose then that $m=4$ with $p$ odd. Then Lemma 7 applies and we find $rs=4p^2-1$,

$$rc^2-2p^2d^2 = a^2$$

$$2c^2-sd^2 = b^2,$$

with $a$, $b$, $c$ and $d$ all odd and coprime in pairs. Then $r\equiv 3 \pmod 8$ and $r$ has only factors $\equiv 1$ or $3 \pmod 8$, $s$ has only factors $\equiv 1$ or $7 \pmod 8$ and $(r \mid p)=1$ if $p$ is odd, and again the theorem follows.

Finally the case $p=m=3$ cannot occur. for now Lemma 6 would apply with $rs=35$ and

$$rc^2-3\mu^2d^2 = a^2$$

$$3\lambda^2c^2-sd^2 = b^2.$$

Since $5 \mid rs$, one of these is impossible modulo 5.

In exactly the same way we may prove the following results whose proofs are omitted.

THEOREM 5. *If $n=8p$, where $p$ denotes a prime, a necessary condition for* (2) *to have solutions is that there exists a factorisation* $16p^2-1=rs$ *with* $(r \mid p)=1$, *if $p$ is odd, and with $r$ not a square, every factor of $r$ congruent to* 1 *modulo* 4. *In particular* $\varrho(1)+\varrho(5)\geqq 1$.

THEOREM 6. *If $n=16p$, where $p$ denotes a prime, a necessary condition for* (2) *to have solutions is that there exists a factorisation* $64p^2-1=rs$ *with $r$ not a square,* $r\equiv 1 \pmod 8$ *and with* $(r \mid p)=1$ *if $p$ is odd and with*

*either* (a) *every factor of $r$ congruent to* 1 *modulo* 4,
*or* (b) *every factor of $r$ congruent to* 1 *or* 3 *modulo* 8 *and every factor of $s$ congruent to* 1 *or* 7 *modulo* 8.

*In particular* $\varrho(1)\geqq 1$ *or* $\varrho(5)\geqq 2$, *or* $\{\varrho(5)=0$ *and* $R(3)$ *is even*$\}$.

THEOREM 7. *If $n=3p$, where $p$ denotes an odd prime, then a necessary condition ofr* (2) *to have solutions is that there exists a factorisation* $9p^2-4=rs$, *where* $(r,s)$ *is divisible only by primes congruent to* 1 *modulo* 4 *and*

*either* (a) $(r \mid p)=1$, $r\equiv 1 \pmod{24}$, *$r$ not a square, every factor of $r$ congruent to* 1 *modulo* 4;

*or* (b) $(2r \mid p)=1$, $r \equiv 5 \pmod{24}$, *every factor of r is conruent to* 1, 5, 7 *or* 11 (mod 24) *and every factor of s is congruent to* $\pm 1$ *or* $\pm 5$ (mod 24);

*or* (c) $(r \mid p)=1$, $r \equiv 7 \pmod{24}$, *every factor of r is congruent to* 1 *modulo* 3 *and every factor of s is congruent to* $\pm 1$ (mod 12);

*or* (d) $(2r \mid p)=1$, $r \equiv 11 \pmod{24}$, *every factor of r is congruent to* 1 *or* 3 *modulo* 8 *and every factor of s is congruent to* 1 *or* 3 *modulo* 8 *and every factor of s is congruent to* 1 *or* 7 *modulo* 8.

Using the above results, we find that no solutions exist for $n=1, 3, 4, 6, 7, 8, 10, 11, 12, 13, 15, 16, 17, 21, 23, 26, 31, 39, 40, 41, 47, 48, 52, 59, 68, 69, 73, 74, 86, 92, 93$ or 97. On the other hand, we find solutions for many values of $n \leqq 100$, and a table of minimal solutions for 53 different values of $n$ is appended (Table 1). This leaves 14 values of $n \leqq 100$, and in fact we are able to show that there are no solutions for any of these; thus the table gives a complete list of values of $n$ for which solutions exist and $n \leqq 100$. The methods used for these 14 values vary in complexity, and it is hoped in a subsequent paper to deal with one of these, $n=49$, in detail.

**Acknowledgement.**

Theorem 3 was first proved by Veluppillai [2], who also calculated many of the solutions given in the table.

## REFERENCES

1. H. C. Pocklington, *Some diophantine impossibilities*, Proc. Cambridge Philos. Soc. 17 (1914), 110–118.
2. M. Veluppillai, *Some diophantine equations*, Ph. D. thesis, University of London, 1977.

ROYAL HOLLOWAY COLLEGE
EGHAM
SURREY TW20 0EX
ENGLAND

Table 1. *Values of* $n \leqq 100$, *for which* (2) *has solutions.*

| $n$ | $x$ | $y$ |
|---|---|---|
| 5 | 3 | 1 |
| 9 | 4 | 1 |
| 14 | 5 | 1 |
| 19 | 7 | 3 |
| 20 | 6 | 1 |
| 22 | 5 | 2 |
| 24 | 7 | 2 |
| 25 | 11 | 4 |
| 27 | 7 | 1 |
| 28 | 4 | 1 |
| 29 | 2967 | 517 |
| 33 | 19 | 1 |
| 34 | 35 | 13 |
| 35 | 8 | 1 |
| 37 | 16 | 5 |
| 38 | 34 | 1 |
| 43 | 5365 | 976 |
| 44 | 9 | 1 |
| 46 | 35 | 17 |
| 51 | 209 | 25 |
| 53 | 13 | 8 |
| 54 | 10 | 1 |
| 55 | 63 | 13 |
| 56 | 24 | 11 |
| 57 | 209 | 29 |
| 58 | 13 | 2 |
| 60 | 18 | 7 |
| 61 | 23 | 3 |
| 63 | 8 | 3 |
| 65 | 11 | 1 |
| 66 | 51 | 5 |
| 67 | 22631 | 1360 |
| 71 | 41 | 1 |
| 75 | 13 | 4 |
| 76 | 195 | 8 |
| 77 | 12 | 1 |
| 78 | 111 | 1 |
| 79 | 267 | 133 |
| 80 | 20 | 1 |
| 81 | 12299 | 1924 |
| 82 | 13 | 3 |
| 83 | 91039 | 42304 |
| 84 | 187 | 3 |
| 85 | 76 | 1 |
| 87 | 32683 | 2928 |
| 88 | 217 | 30 |
| 89 | 26381 | 18040 |
| 90 | 13 | 1 |
| 91 | 21 | 1 |
| 94 | 9605 | 91 |
| 95 | 11 | 3 |
| 96 | 17 | 3 |
| 99 | 19 | 5 |