ON PYTHAGOREAN TRIPLES CONTAINING A FIXED INTEGER

AMITABHA TRIPATHI

Abstract. For a given positive integer n, we determine explicit formulas for the number of occurrences of n as a part of a Pythagorean triple, and also as a part of a primitive Pythagorean triple. We also determine the least positive integer that is a part of at least n such primitive triples and obtain several conditions that help in characterizing the analogous case for all triples.

1. Introduction

Pythagorean triples $\{a, b, c\}$ are positive integers a, b, c which satisfy the equation $a^2+b^2 = c^2$. An *ordered* Pythagorean triple (a, b, c) is a triple that also satisfies the order relation $a < b < c$. For any $k \in \mathbb{N}$ and for any Pythagorean triple $\{a, b, c\}$, the triple $\{ka, kb, kc\}$ is also Pythagorean. A Pythagorean triple $\{a, b, c\}$ is *primitive* if $\gcd(a, b, c) = 1$. All primitive Pythagorean triples (a, b, c) are given parametrically by

$$\{a, b\} = \{r^2 - s^2, 2rs\}, \quad c = r^2 + s^2,$$

where r, s are positive integers of opposite parity, $r > s$, and $\gcd(r, s) = 1$. It can be easily deduced that all Pythagorean triples (a, b, c) can be characterized by

$$\{a, b\} = \{k(r^2 - s^2), 2krs\}, \quad c = k(r^2 + s^2),$$

where r, s are positive integers of opposite parity, $r > s$, and $\gcd(r, s) = 1$ and $k = \gcd(a, b, c)$. All this is well-known and can be found in most books on elementary Number Theory.

The parametric solution to $x^2 + y^2 = z^2$ helps in suggesting and proving several properties that Pythagorean triples satisfy, for instance that $60 \mid abc$ whenever $\{a, b, c\}$ is a Pythagorean triple. It is not difficult to show that for every $n \geq 3$, there is a Pythagorean triple $\{a, b, n\}$. In fact, for each such $n \geq 1$, there are *at least* n Pythagorean triples having the same least member. The main purpose of this article is to determine the number $\mathscr{P}(n)$ (respectively, $\mathscr{P}^\star(n)$) of Pythagorean (respectively, primitive Pythagorean) triples (a, b, c) with $n \in \{a, b, c\}$. This naturally leads us to determine $\ell(n)$ (respectively, $\ell^\star(n)$) which represents the least positive integer that is a member of *at least* n Pythagorean (respectively, primitive Pythagorean) triples. The problem about determining $\mathscr{P}(n)$ and $\mathscr{P}^\star(n)$ is also considered in [4] and about determining $\ell(n)$ in [2]. Lambek & Moser in [5] showed that if $P(N)$ denotes the number of primitive Pythagorean triples $\{a, b, c\}$, $a \leq b \leq c$ and $\frac{1}{2}ab \leq N$, then

$$P(N) = cN^{1/2} + O\big(N^{1/3}\big),$$

where $c = (\pi^5)^{-1/2}\Gamma^2(\frac{1}{4}) \approx 0.53134$, and conjectured that

$$P(N) = cN^{1/2} - c'N^{1/3} + o\big(N^{1/3}\big),$$

where $c' \approx 0.295$.

2. Counting Primitive Pythagorean Triples

We begin by proving the two results related to our main problem that are mentioned in the Introduction. Each proof is constructive and easy to verify.

Lemma 1. *For each $n \geq 3$, there exists a Pythagorean triple $\{a, b, n\}$.*

Proof. Let $n \geq 3$. We show that the equation $a^2 + n^2 = b^2$ has a solution in positive integers $\{a, b\}$. Set $b - a = 1$, $b + a = n^2$ if n is *odd*, and $b - a = 2$, $b + a = \frac{n^2}{2}$ if n is *even*. This gives the triples

$$\begin{cases} \left(n, \frac{1}{2}(n^2 - 1), \frac{1}{2}(n^2 + 1)\right) & \text{when } n \text{ is } \textit{odd}; \\ \left(n, \frac{1}{4}n^2 - 1, \frac{1}{4}n^2 + 1\right) & \text{when } n \text{ is } \textit{even}. \end{cases}$$

This construction completes the proof. □

Lemma 2. *For each $n \geq 1$ and $a \geq 2$, there exists n Pythagorean triples $(2a^n, b_k, c_k)$ for $0 \leq k \leq n - 1$.*

Proof. For $0 \leq k \leq n - 1$, set $b_k = a^k(a^{2n-2k} - 1)$ and $c_k = a^k(a^{2n-2k} + 1)$. Then $c_k^2 - b_k^2 = a^{2k} \cdot 4a^{2n-2k} = (2a^n)^2$. □

Lemma 1 ensures that every n is a part of some primitive Pythagorean triple, so that $\mathscr{P}^\star(n) \geq 1$ for $n \geq 3$. Lemma 2 says that, for each $n \geq 1$, there is some m for which $\mathscr{P}(m) \geq n$. In view of (1), it is convenient to determine $\mathscr{P}^\star(n)$ by looking at the two cases — (i) n even; (ii) n odd.

Theorem 1. *If n is even, then*

$$\mathscr{P}^\star(n) = \begin{cases} 2^{\omega(n)-1} & \textit{if } 4 \mid n; \\ 0 & \textit{if } 4 \nmid n, \end{cases}$$

where $\omega(n)$ is the number of prime divisors of n.

Proof. From (1), if $\{a, b, n\}$ is a primitive Pythagorean triple and n is even, then $n = 2rs$ for some r, s of opposite parity and coprime. Each such pair $\{r, s\}$ uniquely determine the pair $\{a, b\}$. Since rs is even, there is no solution unless $4 \mid n$. Suppose $4 \mid n$, and suppose r is even, without loss of generality. If $\mathbb{P}(n)$ denotes the set of *odd* prime divisors of n, any subset (including $\emptyset$) of $\mathbb{P}(n)$ uniquely determines r, and hence s, since no prime p_i can divide both r and s. There are $2^{\omega(n)-1}$ choices for r, and hence as many choices for expressing n in the form $2rs$ with r, s coprime and of opposite parity. □

The case of odd n requires us to further consider two subcases. Accordingly, let $\mathscr{P}_1^\star(n)$ denote the number of primitive Pythagorean triples $\{a, b, n\}$ where $n < \max\{a, b\}$, and let $\mathscr{P}_2^\star(n)$ denote the number of such triples with $n > \max\{a, b\}$.

Theorem 2. *For odd n,*

$$\mathscr{P}_1^\star(n) = 2^{\omega(n)-1},$$

where $\omega(n)$ is the number of prime divisors of n. Also, $\mathscr{P}_1^\star(1) = 0$.

Proof. We wish to count the number of positive integer pairs $\{r, s\}$ such that $r^2 - s^2 = n$ with r, s of opposite parity and $\gcd(r, s) = 1$. The parity of n forces both factors $r + s, r - s$ to be odd, so that r, s are of opposite parity. Moreover, $\gcd(r, s) = 1$ implies $\gcd(r + s, r - s) = 1$.

So, as in the proof of Theorem 1, choosing the prime factors for one of $r+s, r-s$ determines the prime factors of the other, and r, s are uniquely determined from $r+s, r-s$. However, since we must reserve the larger factor of n for $r+s$, only half of all the subsets count. □

Theorem 3. *For odd n,*

$$\mathscr{P}_2^\star(n) = \begin{cases} 2^{\omega(n)-1} & \text{if no prime of the form } 4k+3 \text{ divides } n; \\ 0 & \text{if } n \text{ has a prime divisor of the form } 4k+3, \end{cases}$$

where $\omega(n)$ is the number of prime divisors of n. Also, $\mathscr{P}_2^\star(1) = 0$.

For a proof of Theorem 3, we refer to [7, pp. 166-167]. The number of solutions in the reference is $2^{\omega_1(n)+2}$, where $\omega_1(n)$ denotes the number of prime divisors of n of the form $4k+1$. However, that counts the number of ways of expressing n as a sum of the squares of two coprime integers, counting all permutations and changes of sign as different representations. Theorems 2 and 3 combine to complete the solution of $\mathscr{P}^\star(n)$ in the case where n is odd.

Theorem 4. *For odd n,*

$$\mathscr{P}^\star(n) = \begin{cases} 2^{\omega(n)} & \text{if no prime of the form } 4k+3 \text{ divides } n; \\ 2^{\omega(n)-1} & \text{if } n \text{ has a prime divisor of the form } 4k+3, \end{cases}$$

where $\omega(n)$ is the number of prime divisors of n. Also, $\mathscr{P}^\star(1) = 0$.

3. Counting Pythagorean Triples

We now turn to the problem of counting Pythagorean triples. Let $d \mid n$, with $n = kd$. Each primitive Pythagorean triple $\{a', b', d\}$ gives rise to a Pythagorean triple $\{ka', kb', n\}$. In view of (2), we therefore have

$$\mathscr{P}(n) = \sum_{d|n} \mathscr{P}^\star(d), \tag{1}$$

and Theorems 1 and 4 of Section 1 may be used to determine $\mathscr{P}(n)$ completely. However, we attempt to solve this problem more directly, without resorting to the results concerning $\mathscr{P}^\star(n)$. Analogous to the definitions in the previous section, we let $\mathscr{P}_1(n)$ (respectively, $\mathscr{P}_2(n)$) denote the number of Pythagorean triples $\{a, b, n\}$ where $n < \max\{a, b\}$ (respectively, $n > \max\{a, b\}$).

Theorem 5. *Let $n \in \mathbb{N}$. The number of ordered pairs (x, y) of positive integers such that $x^2 - y^2 = n$ equals*

$$\begin{cases} \left\lceil \frac{1}{2}\big(d(n) - 1\big) \right\rceil & \text{if } n \text{ is odd}; \\ \left\lceil \frac{1}{2}\big(d\left(\frac{n}{4}\right) - 1\big) \right\rceil & \text{if } 4 \mid n, \end{cases}$$

where $d(n)$ denotes the number of positive divisors of n. Moreover, there is no solution if $n \equiv 2 \pmod 4$.

Proof. Observe that $x^2 - y^2$ has two factors $x-y$, $x+y$ of the same parity. Hence $x^2 - y^2 = n$ has a solution if and only if *either* n is odd *or* n is a multiple of 4.

If n is odd and $n = ab$ with $1 \le a < b \le n$, we may set $x - y = a$ and $x + y = b$ to get $x = \frac{1}{2}(b+a)$ and $y = \frac{1}{2}(b-a)$. Since each divisor a may be paired with its conjugate divisor $\frac{n}{a}$, there are $\frac{1}{2}d(n)$ solutions *unless* n is a square. If $n = m^2$, the factorization $n = m \cdot m$ does not give rise to a valid solution since $y = 0$, so the number of solutions is $\frac{1}{2}\big(d(n) - 1\big)$.

If $4 \mid n$, $n = ab$ with a, b of the same parity and $a \neq b$, we must have a, b both even. So in this case, we are looking at factoring $\frac{n}{4}$ into two *unequal* factors. The number of such solutions, as resolved in the previous case, is obtained by replacing n by $\frac{n}{4}$. This ends the proof. □

Theorem 6. *Let $n \in \mathbb{N}$. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, with $p_1 < p_2 < \cdots < p_k$, the number of Pythagorean triples $\{a, b, n\}$, where $3 \leq n < \max\{a, b\}$, is given by*

$$\mathscr{P}_1(n) = \begin{cases} \frac{1}{2}\Big\{(2e_1+1)(2e_2+1)(2e_3+1)\cdots(2e_k+1) - 1\Big\} & \text{if } n \text{ is odd;} \\ \frac{1}{2}\Big\{(2e_1-1)(2e_2+1)(2e_3+1)\cdots(2e_k+1) - 1\Big\} & \text{if } n \text{ is even.} \end{cases}$$

Moreover, $\mathscr{P}_1(1) = \mathscr{P}_1(2) = 0$.

Proof. Observe that $\mathscr{P}_1(n)$ counts the number of Pythagorean triples $\{a, b, n\}$ where $n < \max\{a, b\}$. This amounts to counting the number of solutions (a, b) of $a^2 - b^2 = n^2$, and Theorem 5 together with the formula for $d(n)$ provides the result. □

The number of ways of expressing n as a sum of two squares, counting all permutations and changes of sign as different representations, equals $4\big(d_1(n) - d_3(n)\big)$, where $d_i(n)$ is the number of positive divisors of n of the form $4k + i$; see [7, pp. 166-167] for details.

Theorem 7. *Let $n \in \mathbb{N}$. If $n = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}$, where each prime $p_i \equiv 1 \pmod 4$ and each prime $q_i \equiv 3 \pmod 4$, the number of Pythagorean triples $\{a, b, n\}$, where $n > \max\{a, b\}$ is given by*

$$\mathscr{P}_2(n) = \frac{1}{2}\Big\{(2e_1+1)(2e_2+1)\cdots(2e_r+1) - 1\Big\}.$$

Proof. Recall that $\mathscr{P}_2(n)$ counts the number of Pythagorean triples $\{a, b, n\}$ where $n > \max\{a, b\}$. This amounts to counting the number of solutions $\{a, b\}$ of $a^2 + b^2 = n^2$ with $a, b \in \mathbb{N}$. By the result referenced to in the paragraph immediately preceding this Theorem, we know this to equals $4\big(d_1(n^2) - d_3(n^2)\big)$, where $d_i(n)$ is the number of positive divisors of n of the form $4k + i$. However, all permutations and changes of sign count as different representations in this formula, and 0 is counted. Hence, with $1 \leq a < b$, we get $\mathscr{P}_2(n) = \frac{1}{2}\big(d_1(n^2) - d_3(n^2) - 1\big)$.

Let $n = 2^e n_1 n_2$, where $n_1 = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $n_2 = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}$, with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$. We have $d_1(n^2) - d_3(n^2) = d(n_1^2)\big\{d_1(n_2^2) - d_3(n_2^2)\big\}$ since each divisor of n_1^2 is of the form $4k + 1$ and does not affect the difference $d_1 - d_3$. There is a one-to-one correspondence between the divisors of n_2^2 and the set of all s-tuple $(v_1, v_2, \ldots, v_s)$, with $0 \leq v_j \leq 2f_j$ for $1 \leq j \leq s$. If we list these s-tuples in order, $(0, 0, 0, \ldots, 0), (1, 0, 0, \ldots, 0), \ldots, (2f_1, 0, 0, \ldots, 0)$, $(2f_1, 1, 0, \ldots, 0), \ldots, (2f_1, 2f_2, 2f_3, \ldots, 2f_s)$, we observe that the divisors alternate between the forms $4k + 1$ and $4k + 3$, starting and ending with divisors of the form $4k + 1$. Hence $d_1(n_2^2) - d_3(n_2^2) = 1$, so that $d_1(n^2) - d_3(n^2) = d(n_1^2)$. This proves the result. □

Theorems 6 and 7 together complete the solution of $\mathscr{P}(n) = \mathscr{P}_1(n) + \mathscr{P}_2(n)$ in all cases. We record this in our next result.

Theorem 8. *For $n \geq 3$, let n_1 denote the largest odd divisor of n each of whose prime divisors is of the form $4k+1$, with $n_1 = 1$ if no such prime divisor exists. Then*

$$\mathscr{P}(n) = \begin{cases} \dfrac{1}{2}\left\{d(n^2) + d(n_1^2)\right\} - 1 & \text{if } n \text{ is odd;} \\ \\ \dfrac{1}{2}\left\{d((\frac{n}{2})^2) + d(n_1^2)\right\} - 1 & \text{if } n \text{ is even,} \end{cases}$$

where $d(n)$ denotes the number of positive divisors of n. Moreover, $\mathscr{P}(1) = \mathscr{P}(2) = 0$.

We note that Theorem 8 implies

$$\mathscr{P}(2^e) = e - 1, \quad \mathscr{P}(p^e) = 2e, \quad \mathscr{P}(q^e) = e, \tag{2}$$

if p and q are primes with $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. In fact, 2^{e+1} and q^e are interchangeable in the formula for $\mathscr{P}(n)$ since both contribute equally to the sum in $\mathscr{P}(n)$. We close this section with the following easy but useful consequence of Theorem 8.

Corollary 1. *If m is odd and $e \geq 1$, then*

$$\mathscr{P}(2^e\, m) = \mathscr{P}(m) + (e-1) \cdot d(m^2).$$

Proof. Let m be odd and $e \geq 1$. Observe that the largest divisors each of whose prime factors is of the form $4k+1$ of $2^e\, m$ and m are equal; set this divisor as m_1. From Theorem 8 we have

$$\mathscr{P}(2^e\, m) - \mathscr{P}(m) = \frac{1}{2}\big\{(2e-1)\, d(m^2) + d(m_1^2)\big\} - \frac{1}{2}\big\{d(m^2) + d(m_1^2)\big\} = (e-1) \cdot d(m^2).$$

□

4. Optimal $\mathscr{P}$-numbers

In this closing section we extend the results of Sections 2 and 3. For each $n \in \mathbb{N}$, we seek the *least* positive integer $\ell(n)$ (respectively, $\ell^\star(n)$) such that there are *at least* n Pythagorean (respectively, primitive Pythagorean) triples $\{a, b, n\}$. Lemma 2 not only guarantees the existence of $\ell(n)$ but also shows that $\ell(n) \leq 2^{n+1}$.

Theorem 9. *Let $n \in \mathbb{N}$, and let k be such that $2^{k-1} < n \leq 2^k$. Let $\ell^\star(n)$ denote the least positive integer that is a member of (at least) n primitive Pythagorean triples. Then, for $n \geq 3$,*

$$\ell^\star(n) = 4p_1p_2 \cdots p_k,$$

where p_i is the ith odd prime. Moreover, $\ell^\star(1) = 3$ and $\ell^\star(2) = 5$.

Proof. Fix $n \in \mathbb{N}$. We recall that $\mathscr{P}^\star(m)$ is always a power of 2 by Theorems 1 and 4. Let k be such that $2^{k-1} < n \leq 2^k$. Suppose m is even and $\mathscr{P}^\star(m) \geq 2^k$. From Theorem 1 any minimum m must satisfy $4 \mid m$ and $\omega(m) - 1 = k$. This is achieved with $m = 4p_1p_2 \cdots p_k$, where p_i is the ith odd prime. If m is odd and $\mathscr{P}^\star(m) \geq 2^k$, we consider two cases. The minimum among m which have at least one prime divisor of the form $4k+3$ is $p_1p_2 \cdots p_kp_{k+1}$ by Theorem 4. The minimum among m all of whose prime divisors are of the form $4k+1$ is $p_1'p_2' \cdots p_k'$, where p_i' denotes the ith prime of the form $4k+1$. Therefore, the minimum m for which $\mathscr{P}^\star(m) \geq n$ is

$$\min\{4p_1p_2 \cdots p_k, p_1p_2 \cdots p_kp_{k+1}, p_1'p_2' \cdots p_k'\} = 4p_1p_2 \cdots p_k,$$

except that the minimum is 3 when $k = 0$ (so $n = 1$) and 5 when $k = 1$ (so $n = 2$). This completes the proof. □

The following definition is useful in restating the result in Theorem 9 and also in the determination of $\ell(n)$.

Definition 1. *Let $m_0 \in \mathbb{N}$. We say that m_0 is an* optimal $\mathscr{P}$-number *(respectively,* optimal $\mathscr{P}^\star$-number*) provided $\mathscr{P}(m_0) > \mathscr{P}(m)$ (respectively, $\mathscr{P}^\star(m_0) > \mathscr{P}^\star(m)$) whenever $1 \leq m < m_0$.*

Theorem 9 states that the sequence of optimal $\mathscr{P}^\star$-numbers, with their $\mathscr{P}^\star$-values, is given by

$$\mathscr{P}^\star(3) = 1, \quad \mathscr{P}^\star(5) = 2, \quad \mathscr{P}^\star(4p_1p_2\cdots p_k) = 2^k \text{ for } k \geq 2$$

where p_i denotes the ith odd prime.

The optimal $\mathscr{P}$-numbers are reminiscent of "highly composite numbers", introduced by Ramanujan, to study numbers that have a larger number of divisors than any number less than it. We explore the problem of determining $\ell(n)$ by providing some necessary conditions for the sequence of optimal $\mathscr{P}$-numbers. In order to study the optimal $\mathscr{P}$-numbers, we not only make repeated use of Theorem 8, but also its two Corollaries. The following result puts together some necessary conditions that the prime factorization of optimal $\mathscr{P}$-numbers satisfy. However, there does not seem to be a nice formulation for $\ell(n)$ or even for optimal $\mathscr{P}$-numbers, unlike the analogous case for primitive Pythagorean triples.

Lemma 3. *Let n, k be integers, with $0 \leq k \leq n$, and let $c \in \mathbb{R}^+$. Consider the function*

$$f(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} x_i + \prod_{i=1}^{k} x_i,$$

with each $x_i > 0$ and such that $x_1 + x_2 + \cdots + x_n = c$, and where we use the usual convention that the empty product equals 1. Then f has a maximum when

(a) *$x_i = c/n$ for $1 \leq i \leq n$, provided $k = 0$ or $k - n$;*
(b) *$x_i = x$ for $1 \leq i \leq k$, $x_i = y$ for $k + 1 \leq i \leq n$, and*

$$(c - nx)y^{n-k-1} + (n - k) = 0,$$

provided $1 \leq k \leq n - 1$.

Proof.

(a) Observe that both $k = 0$ and $k = n$ reduce to the problem of maximizing the product of n positive numbers whose sum is fixed. From the Arithmetic Mean-Geometric Mean inequality, this occurs precisely when all x_i's are equal.
(b) Let $1 \leq k \leq n - 1$. If D_i denotes the partial derivative of f with respect to x_i, then setting $D_1 = D_2 = \cdots = D_k$ gives $x_1 = x_2 = \cdots = x_k = x$ (say), and $D_{k+1} = D_{k+2} = \cdots = D_n$ gives $x_{k+1} = x_{k+2} = \cdots = x_n = y$. For this extrema, $kx + (n - k)y = c$. If we now set

$$F(x) = \frac{1}{(n-k)^{n-k}} x^k (c - kx)^{n-k} + x^k,$$

a routine computation shows the condition on the extremum for the function F is

$$(c - nx)y^{n-k-1} + (n - k) = 0.$$

□

Theorem 10. *Suppose $p_1, p_2, \ldots, p_r$ are primes of the form $4k + 1$ and $q_1, q_2, \ldots, q_s$ are primes of the form $4k + 3$. Among all N of the form $2^e \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j}$ with $\sum_{i=1}^{r} \alpha_i + \sum_{j=1}^{s} \beta_j$ fixed, any one with largest $\mathscr{P}$-value satisfies $|\alpha_i - \alpha_j| \leq 1$ and $|\beta_i - \beta_j| \leq 1$, for each $i \neq j$.*

Proof. Consider any N of the form $2^e \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j} = 2^e m$ with $\sum_{i=1}^{r} \alpha_i + \sum_{j=1}^{s} \beta_j$ fixed. Since $2\alpha_1 + 1, \ldots, 2\alpha_r + 1, 2\beta_1 + 1, \ldots, 2\beta_s + 1$ has a fixed sum, its product $d(m^2)$ is maximum when the terms are chosen as equal as possible. Thus $|\alpha_i - \alpha_j| \leq 1$ and $|\beta_i - \beta_j| \leq 1$ for $i \neq j$, and by Corollary 1, it is sufficient to prove the assertion for *odd* N. For the rest of the proof, we assume $e = 0$.

From Theorem 8,

$$2\{\mathscr{P}(N) + 1\} = d(N^2) + d(N_1^2) = \prod_{i=1}^{r}(2\alpha_i + 1) \prod_{j=1}^{s}(2\beta_j + 1) + \prod_{i=1}^{r}(2\alpha_i + 1).$$

In order to maximize $\mathscr{P}(N)$, by Lemma 3 we must choose the terms from each of the sequences $\{2\alpha_i + 1\}_{i=1}^{r}$, $\{2\beta_j + 1\}_{j=1}^{s}$ as equal as possible. This completes the proof of our assertion. □

We are now in a position to state our final result about optimal $\mathscr{P}$-numbers.

Theorem 11. *Let*

$$N = 2^e p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

be the prime factor decomposition of an optimal $\mathscr{P}$-number, where $\{p_i\}_{i=1}^{r}$ is an increasing sequence of primes of the form $4k+1$ and $\{q_j\}_{j=1}^{s}$ is an increasing sequence of primes of the form $4k + 3$. Then

(a) *each of the sequences $\{\alpha_i\}_{i=1}^{r}$ and $\{\beta_j\}_{j=1}^{s}$ is nonincreasing. Moreover, $\alpha_1 - \alpha_r \leq 1$, $\beta_1 - \beta_s \leq 1$, and if N is even, then $e \geq 1 + \max\{\alpha_1, \beta_1\}$;*
(b) *the sequence of primes $\{p_1, p_2, \ldots, p_r\}$ and $\{q_1, q_2, \ldots, q_s\}$ are consecutive;*
(c) *each prime less than q_s and of the form $4k + 1$ is a divisor of N;*
(d) *each prime less than p_k and of the form $4k + 3$ is a divisor of N, where p_k is the largest prime for which $p_k^2 \mid N$;*
(e) *if N is odd, then $N \in \{3, 5, 15\}$;*
(f) *if N is even, then $60 \mid N$ except if $N \in \{12, 24, 40, 48\}$.*

Proof. Throughout this proof, we assume that N is an optimal $\mathscr{P}$-number with the prime factorization as stated in the theorem.

(a) Suppose $N = mp_i^{\alpha_i} p_j^{\alpha_j}$, with $p_i < p_j$ and $\alpha_i > \alpha_j$. Then $N' = mp_i^{\alpha_j} p_j^{\alpha_i} < N$ and $\mathscr{P}(N') = \mathscr{P}(N)$ proves that N cannot be an optimal $\mathscr{P}$-number. The same argument carries over if we replace p_i, p_j by q_i, q_j.

The condition on the difference between the largest and smallest exponents for both sequences $\{\alpha_i\}_{i=1}^{r}$ and $\{\beta_j\}_{j=1}^{s}$ follow from Theorem 10. If N is even, observe that replacing either a q_1 by a 2 or a p_1 by a 2^2 results in a smaller number with at least as large a $\mathscr{P}$-value provided $e \leq \beta_1$ and $e \leq \alpha_1$.

(b) Suppose $p \mid N$, $p' \nmid N$ for primes p', p with $p' < p$ and $p' \equiv p \pmod 4$. If $N = mp^\alpha$, where $p \nmid m$, then $N' = mp'^\alpha < N$ satisfies $\mathscr{P}(N') = \mathscr{P}(N)$, thereby proving that N cannot be an optimal $\mathscr{P}$-number.

(c) Suppose $p < q_s$ is prime of the form $4k+1$. If $p \nmid N$, replacing a factor q_s of N by p results in a smaller number with a larger $\mathscr{P}$-value. So N must be divisible by each of the prime factors of the form $4k+1$ that are less than q_s.

(d) Suppose p_k is the largest prime such that $p_k^2 \mid N$. If $q < p_k$ is prime of the form $4k+3$ and $q \nmid N$, replacing a factor p_k of N by q results in a smaller number with a larger $\mathscr{P}$-value. So N must be divisible by each of the prime factors of the form $4k+3$ that are less than p_k.

(e) Suppose N is odd and $N \notin \{3, 5, 15\}$. If N has at least two prime factors of the form $4k+3$, not necessarily distinct, replacing these by 2^2 results in a smaller number with at least as large a $\mathscr{P}$-value. Otherwise, replacing any two prime factors of N by 2^3 again produces a smaller number with at least as large a $\mathscr{P}$-value. This proves our assertion.

(f) Suppose N is even. Then $4 \mid N$ since $\mathscr{P}(2m) = \mathscr{P}(m)$ for odd m. Also, N cannot be a power of 2 since $9e - 40 = \mathscr{P}(2^{e-4} \cdot 3 \cdot 5) > \mathscr{P}(2^e) = e - 1$ for $e \geq 5$, and since $\mathscr{P}(1) = \mathscr{P}(2)$, $\mathscr{P}(3) = \mathscr{P}(4)$, $\mathscr{P}(5) = \mathscr{P}(8)$ and $\mathscr{P}(15) > \mathscr{P}(16)$. By parts (b), (c) and (d), if N has only one odd prime divisor, that must be either 3 or 5, and if N has at least two odd prime divisors, both 3 and 5 must divide N. Thus we are done except for proving the exceptional cases.

We now show that if N is of the form $2^e \cdot 3^f$ or $2^e \cdot 5^f$, then $f = 1$. To do this, it is enough to show that $f \leq 1$ in each case. Indeed, if $f \geq 2$, replacing a $2 \cdot 3$ by 5 in the first case and replacing a $2 \cdot 5$ by 7 in the second case results in a smaller number with larger $\mathscr{P}$-value. Thus N must be of the form $2^e \cdot 3$ or $2^e \cdot 5$.

If $N = 2^e \cdot 3$ and $e \geq 5$, replacing 2^3 by 5 results in a smaller number with a larger $\mathscr{P}$-value. Each of the numbers $2^e \cdot 3$, $2 \leq e \leq 4$, is optimal, as can be verified. If $N = 2^e \cdot 5$ and $e \geq 4$, replacing 2^2 by 5 results in a smaller number with a larger $\mathscr{P}$-value, and it can be verified that only $2^3 \cdot 5$ is optimal.

□

We close this article with a list of the optimal $\mathscr{P}$-numbers less than 10000.

n	**prime factorization of** n	$\mathscr{P}(n)$
3	3	1
5	5	2
12	$2^2 \cdot 3$	4
15	$3 \cdot 5$	5
24	$2^3 \cdot 3$	7
40	$2^3 \cdot 5$	8
48	$2^4 \cdot 3$	10
60	$2^2 \cdot 3 \cdot 5$	14
120	$2^3 \cdot 3 \cdot 5$	23
240	$2^4 \cdot 3 \cdot 5$	32
360	$2^3 \cdot 3^2 \cdot 5$	38
420	$2^2 \cdot 3 \cdot 5 \cdot 7$	41
720	$2^4 \cdot 3^2 \cdot 5$	53
840	$2^3 \cdot 3 \cdot 5 \cdot 7$	68
1560	$2^3 \cdot 3 \cdot 5 \cdot 13$	71
1680	$2^4 \cdot 3 \cdot 5 \cdot 7$	95
2520	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	113
3360	$2^5 \cdot 3 \cdot 5 \cdot 7$	122
5040	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	158
8400	$2^4 \cdot 3 \cdot 5^2 \cdot 7$	159
9240	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	203

Table of optimal $\mathscr{P}$-numbers less than 10000.

References

[1] R. Amato, *On the Determination of Pythagorean Triples*, Atti Soc. Peloritana Sci. Fis. Mat. Natur., **27** (1981), 3–8.
[2] L. Bernstein, *Primitive Pythagorean Triples*, The Fibonacci Quarterly, **20.3** (1982), 227–241.
[3] J. Duttlinger and W. Schwarz, *Über die Verteilung der Pythagorischen Dreiecke*, Colloq. Math., **43.2** (1980), 365–372.
[4] T. A. Jenkyns and D. McCarthy, *Integers in Pythagorean Triples*, Bull. Inst. Combin. Appl., **4** (1992), 53–57.
[5] J. Lambek and L. Moser, *On the Distribution of Pythagorean Triangles*, Pacific J. Math., **5** (1955), 73–83.
[6] B. V. Love, *On the Classification of Pythagorean Triples*, New Zealand Math. Mag., **13.1** (1976), 9–12.
[7] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley & Sons, 1991.

MSC2000: 11B13

Department of Mathematics, Indian Institute of Technology, Hauz Khas, New Delhi – 110016, India
E-mail address: atripath@maths.iitd.ac.in