Hang Lung Mathematics Awards
Vol. 7 (2016)

Hang Lung Mathematics Awards 2016

Honorable Mention

Triples of Sums of Two Squares

Team members: Kin Ip Mong, Chun Ming Lai, Siu Hong Mak
Teacher: Mr. Chun Yu Kwong
School: Wong Shiu Chi Secondary School

Hang Lung Mathematics Awards
Vol. 7 (2016), pp. 163–200

TRIPLES OF SUMS OF TWO SQUARES

TEAM MEMBERS
Kin Ip Mong, Chun Ming Lai, Siu Hong Mak

TEACHER
Mr. Chun Yu Kwong

SCHOOL
Wong Shiu Chi Secondary School

Abstract. In 1903, an anonymous reader submitted a question to Mathematical Questions in The Educational Times: Find all consecutive triples of sums of two squares. J.E. Littlewood later posed a question on whether in general there exist infinitely many triples n, $n+h$, $n+k$ that are simultaneously sums of two squares? By solving the equation $a^2+2=(a-l)^2+b^2$, we give all consecutive triples of sums of two squares such that the first number is a perfect square. This method is generalised to solve Littlewoods problem for the case when h is a perfect square.

We also prove that there are infinitely many pairs of consecutive triples of sums of two squares such that the first numbers of the two triples differ by 8.

1. Introduction

In 1903, an anonymous reader submitted a question to Mathematical Questions in the British journal The Educational Times: Find all consecutive triples of sums of two squares. Solutions were submitted by A. J. Champneys Cunningham and two other British academics. [8] In 2000, problem A2 of the 61^{st} William Lowell Putnam Mathematical Competition was to show that there exist infinitely many triples $(n, n+1, n+2)$ such that each member of the triple is a sum of two squares. [5][1] This can be easily proved by giving an infinite sequence of triples having the property. $(4n^4+4n^2, 4n^4+4n^2+1, 4n^4+4n^2+2)$ is one of the examples as

$$\begin{cases} 4n^4+4n^2=(2n^2)^2+(2n)^2 \\ 4n^4+4n^2+1=(2n^2+1)^2+0^2 \\ 4n^4+4n^2+2=(2n^2+1)^2+1^2 \end{cases}.$$

[1]For examples, (0,1,2) is the first set of those triples since $0=0^2+0^2$, $1=1^2+0^2$ and $2=1^2+1^2$.

Many solutions of the Putnam problem can be found on the web. All these solutions construct infinitely many such triples. But the triples given in these solutions are all different, and many triples with the property are not included in any of these solutions. The 1903 Educational Times problem is much harder than the 2000 Putnam problem. In our project, we give a partial solution to the 1903 problem, with an additional condition that one of the three numbers of the triple is a perfect square. We also proved that there are infinitely many pairs of consecutive triples of sums of two squares such that their starting numbers differ by 8.

When n is a perfect square, it is obvious that both n and $n+1$ are sums of two squares. We have a triple of the desired property if $n+2$ can be written as the sum of two squares. It leads to our search for the solution to the quadratic Diophantine equation $a^2 + 2 = (a - l)^2 + b^2$. We find that the equation has solutions if and only if all prime factors of l are congruent to 1 or 7 modulo 8, and we can give the general solution of the equation if we have the square roots of 2 modulo l. [See reviewer's comment (1)]

We then further apply our method to the equation $a^2 + k = (a - l)^2 + b^2$ (k is an arbitrary integer). The possible values of l depend on the prime factorization of k. Our work on this equation gives a partial solution to a problem posed by John Edensor Littlewood: Given distinct positive integers h and k, do there exist infinitely many triples $n, n+h, n+k$ that are simultaneously sums of two squares? [8]

2. A Putnam problem

In 2000, a problem appeared in the 61^{st} Williams Lowell Putnam Mathematical Competition:

> Prove that there exist infinitely many integers n such that n, $n+1$ and $n+2$ are each the sum of the squares of two integers. [Example: $0 = 0^2 + 0^2, 1 = 0^2, 1^2, 2 = 1^2 + 1^2$.]

There are many solutions to this statement available on the internet. Most of them take $n+1$ as a perfect square. If $n + 1 = x^2 = x^2 + 0^2$, then $n + 2 = x^2 = x^2 + 1^2$ and what remains is to show that there are infinitely many ways to write $n = x^2 - 1$ as the sum of two squares.

For convenience, we call a triple of non-negative integers $(n, n + h, n + k)$ an h, k-triple if n, $n+h$ and $n+k$ are all sums of two perfect squares. The Putnam problem is to prove that there exist infinitely many 1,2-triples.

2.1. When $n+1$ is a square

Let z be an given even integer. Then $z^2+1=ab$ for some odd integers a and b. By letting $x=\dfrac{a+b}{2}$ and $y=\dfrac{a-b}{2}$, we have $z^2+1=x^2-y^2$. Take $n=x^2-1$, then $n=z^2+y^2$, $n+1=x^2+0^2$.[6][2]

In particular, we can take $a=z^2+1$ and $b=1$. Then $x=\dfrac{z^2}{2}+1$, $y=\dfrac{z^2}{2}$ and hence $n=z^2+\left(\dfrac{z^2}{2}\right)^2$, $n+1=\left(\dfrac{z^2}{2}+1\right)^2+0^2$ and $n+2=\left(\dfrac{z^2}{2}+1\right)^2+1^2$. As $\left(\dfrac{z^2}{2}+1\right)^2$ is a strictly increasing function for positive z, this construction gives infinitely many $1,2$-triples.

Remark 1. *Whenever the middle number of an $1,2$-triple is a perfect square, say x^2, x^2-1 is a sum of two squares. Since $x^2-1=y^2+z^2$ and a perfect square has remainder either 0 or 1 when it is divided by 4, both y and z must be even, as otherwise $x^2=y^2+z^2+1$ will have remainder 2 or 3 when it is divided by 4. [See reviewer's comment (2)] Let $a=x+y$, $b=x-y$. Then $abx^2-y^2=z^2+1$. So the above solution actually gives a method to construct all 1,2-triples with the middle number being a perfect square.*

2.2. 1,2-triples by solutions of a Pells Equation [6]

Pell's equation $x^2-2y^2=1$ has infinitely many solutions. [3] If $n=x^2-1$, then $n=y^2+y^2$, $n+1=x^2+0^2$, $n+2=(y-1)^2+(y+1)^2$. [4]

Remark 2. *As the middle numbers of the 1,2-triples given by this solution are perfect squares, all of them are covered by the solution in Section 2.1. However, the idea of using the solutions of a Pells Equation helps us to prove a property of 1,2-triples in Chapter 3.*

2.3. BrahmaguptaFibonacci Identity

The famous BrahmaguptaFibonacci identity [12]

$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$$

---

[2]The original proof includes a condition that z^2+1 is not prime. This condition is indeed unnecessary.

[3]Let $\begin{pmatrix}x_1\\y_1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$, $\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}=\begin{pmatrix}3&4\\2&3\end{pmatrix}\begin{pmatrix}x_n\\y_n\end{pmatrix}$ for $n\geq 1$. Then $x_n^2-2y_n^2=1$. [2]

[4]The solutions of Pells Equations grow very fast. Among the first 12,095 1,2-triples, this method covers only five of them.

can be used to generate an 1,2-triple from another 1,2-triple. Let $x^2 - 1 = z^2y + 2$ which is the sum of two squares, then

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (z^2 + y^2)(x^2 + 1) = (zx - y)^2 + (yx + z)^2.$$

So $x^4 - 1$ is also the sum of two squares. Therefore $(z^2 + y^2, x^2 + 0^2, x^2 + 1^2)$ induces the 1, 2-triple $((zx - y)^2 + (yx + z)^2, x^4 + 0^2, x^4 + 1^2)$. [6]

2.4. Missing solutions

This Putnam problem may be the easiest one in the 61^{st} competition[5], and there are many ways to give an infinite set of 1,2-triples. Many proofs are available on the internet, but these proofs are quite different and there are many 1,2-triples not covered by any one of the proofs. We used an Excel VBA program to test all non-negative integers up to 4,800,000 and found that there are 977,896 of these integers which can be written as the sum of two perfect squares. Among these integers, 12,095 1,2-triples are found.

While it is not difficult to solve the problem, all those solutions on the internet missed most of the triples found by our computation. Among the first 12,095 1,2-triples, only 107 of them have the middle numbers being perfect squares (0.88%). [6]

3. More about 1,2-triples

3.1. Properties of 1,2-triples

Theorem 3. *An 1,2-triple always starts with a multiple of 8.*

Proof. Let $x = 4n + k$, where $n \in \mathbf{Z}$ and $k \in \{0, 1, 2, 3\}$. Then

$$x^2 = 8(2n^2 + kn) + k^2.$$

So we can find all possible values of x^2 modulo 8 by considering 0^2, 1^2 and 3^2, as shown in TABLE 1. So for $x, y \in \mathbf{Z}$, only possible values of $x^2 + y^2$ modulo 8 are

$x \pmod 4$	0	1	2	3
$x^2 \pmod 8$	0	1	4	1

TABLE 1. All possible values of $x^2 \pmod 8$

0,1,2,4 and 5, as shown in TABLE 2. [See reviewer's comment (3)]

[5] 150 of the top 195 contestants scored full mark in this problem. [7]

[6] We later refine our algorithm and find 3,008,296 1,2-triples, only 1,388 of them have the middle number being perfect squares (0.046%).

$x^2+y^2 \pmod 8$		$x^2 \pmod 8$		
		0	1	4
$y^2 \pmod 8$	0	0	1	4
	1	1	2	5
	4	4	5	0

TABLE 2. All possible values of $x^2 + y^2 \pmod 8$

Therefore, the starting number of an 1,2-triple can only be a multiple of 8. □

Theorem 4. *There are no four consecutive integers such that all of them can be written as the sums of two perfect squares.*

Proof. Direct from TABLE 2. □

Theorem 5. *If* $(n, n+1, n+2)$ *is an* $1,2$*-triple, then* $n \equiv 0,\ 8$ *or* 16 *(mod* 72*).*

Proof. All the possible values of x^2 modulo 9 are shown in TABLE 3.

$x \pmod 9$	0	1	2	3	4	5	6	7	8
$x^2 \pmod 9$	0	1	4	0	7	7	0	4	1

TABLE 3. All possible values of $x^2 \pmod 9$

So for $x, y \in \mathbf{Z}$, only possible values of $x^2 + y^2$ modulo 9 are 0, 1, 2, 4, 5, 7 and 8, as shown in TABLE 4.

$x^2+y^2 \pmod 9$		$x^2 \pmod 9$			
		0	1	4	7
$y^2 \pmod 9$	0	0	1	4	7
	1	1	2	5	8
	4	4	5	8	2
	7	7	8	2	5

TABLE 4. All possible values of $x^2 + y^2 \pmod 9$

Therefore, as the starting number of an $1, 2$-triple,

$$n \equiv 7,\ 8 \text{ or } 0 \pmod 9.$$

By Theorem 3, $n \equiv 0 \pmod 8$.
By Chinese Remainder Theorem[7], the simultaneous linear congruence can be solved and we have

$$n \equiv 0,\ 8 \text{ or } 16 \pmod{72}.$$

□

Theorem 6. *There is no* $1, 2$*-triple in the form of* $(x^2 - 2, x^2 - 1, x^2)$.

Proof. By Theorem 3, $x^2 - 2$ is a multiple of 8 and therefore $x^2 \equiv 2 \pmod 8$, which is impossible (See TABLE 1). □

3.2. Consecutive $1, 2$-triples

Theorem 3 implies that starting numbers of two $1, 2$-triples differ by at least 8. We say that two $1, 2$-triples are consecutive if their starting numbers differ by 8. There are infinitely many pairs of consecutive $1, 2$-triples. [See reviewer's comment (4)]

Theorem 7. *There are infinitely many integers* n *such that al of* n, $n + 1$, $n + 2$, $n + 8$, $n + 9$ *and* $n + 10$ *are sums of two perfect squares.* [8] [9]

Proof. The quadratic Diophantine equation $b^2 - 2a^2 = 9$ has infinitely many solutions[10]. If (a, b) satisfies the relation, then

$$\begin{aligned} 2a^2 &= a^2 + a^2 \\ 2a^2 + 2 &= (a + 1)^2 + (a - 1)^2 \\ 2a^2 + 8 &= (a + 2)^2 + (a - 2)^2 \\ 2a^2 + 9 &= b^2 + 0^2 \\ 2a^2 + 10 &= b^2 + 1^2. \end{aligned}$$

If $2a^2 + 1$ can be written as the sum of two perfect squares, then we have infinitely many integers n such that all of n, $n + 1$, $n + 2$, $n + 8$, $n + 9$ and $n + 10$ are sums of two perfect squares. Note that

$$2a^2 + 1 = \frac{16a^2 + 2a^2 + 9}{9}$$

[7] Theorem 13

[8] The first 4 values of n having this property are 0, 8, 72 and 576.

[9] Theorem 7 was proposed and proved by T. Cochrane, R.E. Dressler. [3] The first 4 values of n given in their proof are 0, 1088 and 39350528 and 1480604673600.

[10] Let $(a_0, b_0) = (0, 3)$ and $a_{n+1} = 3a_n + 2b_n$, $b_{n+1} = 4a_n + 3b_n$ for all nonnegative integers n. Then $b_n^2 - 2a_n^2 = 9$ for all nonnegative integers n.

$$= \frac{16a^2 + b^2}{9}$$
$$= \left(\frac{4a}{3}\right)^2 + \left(\frac{b}{3}\right)^2.$$

All we need to prove is that both a and b are multiples of 3.
Note that $b^2 = 2a^2 + 9 \equiv 2a^2 \pmod 3$.
If a is not a multiple of 3, then $a \equiv -1$ or 1 (mod 3) and hence $2a^2 \equiv 2 \pmod 3$..
It is impossible as b^2 can only be congruent to 0 or 1 modulo 3.
Therefore, a is a multiple of 3 and hence $b^2 = 2a^2 + 9$ is a multiple of 9. So b is also a multiple of 3.[11] □

Theorem 5 suggests that it is impossible to have four consecutive $1, 2$-triples. T. Cochrane, R.E. Dressler pointed out that there are integers k such that $72k$, $72k+1$, $72k+2$, $72k+8$, $72k+9$, $72k+10$, $72k+16$, $72k+17$ and $72k+18$ are all sums of two squares. It is unknown that whether there are infinitely many such values of k. But up to 10200, the only values of k having this property are 0, 2216 and 3872. [3] From the results of our computations, we notice that a k with such property must be a multiple of 8.

Theorem 8. *If n, $n+1$, $n+2$, $n+8$, $n+9$, $n+10$, $n+16$, $n+17$ and $n+18$ are all sum of two squares, then n is a multiple of* 576.

Proof. By Theorem 3, n is a multiple of 8. Refer to TABLE 1 and 2, $n = a^2 + b^2$ for some even integers a and b.
We can write $a = 2(4k + \theta)$ for some integer k and $\theta \in \{0, 1, 2, 3\}$.
Then $a^2 = 4(16k^2 + 8k\theta + \theta^2) \equiv 4\theta^2 \pmod{32}$.

$a \pmod 8$	0	2	4	6
$a^2 \pmod{32}$	0	4	16	4

TABLE 5. All possible values of $a^2 \pmod{32}$

So $a^2 \equiv 0$, 4 or 16 (mod 32).. Similarly, $b^2 \equiv 0$, 4 or 16 (mod 32). and thus as a multiple of $n = a^2 + b^2 \equiv 0$, 8 or 16 (mod 32).

Since $n + 8$ and $n + 16$ are also multiples of 8, we also have

$$\begin{cases} n + 8 \equiv 0, 8, 16 & \pmod{32} \\ n + 16 \equiv 0, 8, 16 & \pmod{32} \end{cases}.$$

Therefore, n must be a multiple of 32 and hence both a and b are multiples of 8. So, n is a multiple of 64.

[11] The first 4 values of n given in this proof are 0, 72 and 2592 and 88200.

$a^2+b^2 \pmod{32}$		$a^2 \pmod{32}$		
		0	4	16
$b^2 \pmod{32}$	0	0	impossible	16
	4	impossible	8	impossible
	16	16	impossible	0

TABLE 6. All possible values of $a^2+b^2 \pmod{32}$

As shown in the proof of Theorem 5, $n \equiv 7, 8, 0 \pmod 9$. This implies that $n+8 \equiv 76, , 8 \pmod 9$ and $n+16 \equiv 5, 6, 7 \pmod 9$. But as $n+8$ and $n+16$ are also starting numbers of $1, 2$-triples, they are both congruent to 7, 8 or 0 modulo 9. So the only possibility is that n is a multiple of 9.
Therefore, n is a multiple of 576. □

While it is unknown whether there exist infinitely many sets of three consecutive $1, 2$-triples, we use an Excel VBA program[12] to find all $1, 2$-triples with numbers in the triples not exceeding $2,147,483,647$. We find $3,008,296$ $1, 2$-triples and they form $58,450$ pairs of consecutive $1, 2$-triples and 244 sets of three consecutive $1, 2$-triples.

4. a^2+2 as the sum of two squares

In Chapter 2, we have a method to find all $1, 2$-triples $(n, n+1, n+2)$ with $n+1$ being a perfect square. It is proved in Chapter 3 that there is no $1, 2$-triple with $n+2$ being a perfect square. [See reviewer's comment (5)] In this chapter, we will give all $1, 2$-triples starting with perfect squares n. If $n = a^2 + 0^2$ for some integer a, then $n+1 = a^2 + 1^2$. We only need to find ways to express a^2+2 as the sum of two squares. This leads to our study of the equation $a^2 + 2 = (a-l)^2 + b^2$. We notice that the solutions to this equation have some patterns. Among all positive integers under 100, only possible values of l are 1, 7, 17, 23, 31, 41, 47, 49, 71, 73, 79, 89, 97. Except 1 and 49, all of these values are prime numbers of forms $8n+1$ or $8n-1$. We find a necessary and sufficient condition on l for the existence of solutions to the equation and give the general solution to it.

4.1. Linear congruence

Definition 9 (Least positive residue)**.** *Let a and m be integers such that $m \geq 2$ and a is not divisible by m. The least positive residue of a modulo m is the integer r such that $1 \leq r \leq m-1$ and $a \equiv r \pmod m$.*

[12]We use the Sum of Two Squares Theorem [19] [1] in our algorithm.

Remark 10. *By Division Algorithm, the least positive residue is well-defined.*

Theorem 11. *Let p be a prime and a be an integer not divisible by p. If R is the set of all least positive residues of $\{a, 2a, 3a, \ldots, (p-1)a\}$ modulo p, then $R = \{1, 2, 3, \ldots, (p-1)\}$.*

Proof. Obviously, $R \subset \{1, 2, 3, \ldots, p-1\}$.
Let $ra, rs \in \{a, 2a, 3a, \ldots, (p-1)a\}$ with $r \geq s$. If $ra \equiv sa \pmod{p}$, then $(r-s)a = ra - sa = np$ for some integer n. Since a is not divisible by p, $r-s$ must be divisible by p. [See reviewer's comment (6)]
As $0 \leq r - s < p$, $r = s$. Therefore, for any two distinct elements of the set $\{a, 2a, 3a, \ldots, (p-1)a\}$, their least positive residues modulo p are different.
So, $|R| = p-1$ and hence the set of all least positive residues of $\{a, 2a, 3a, \ldots, (p-1)a\}$ is $\{1, 2, 3, \ldots, (p-1)\}$. □

Theorem 12. *Let p be a prime and a, b be integers not divisible by p. There exist a unique $x \in \{1, 2, 3, \ldots, (p-1)\}$ such that $ax \equiv b \pmod{p}$.*

Proof. By Division Algorithm, there exists a unique least positive residue b_0 of b modulo p. By Theorem 11, there exists exactly one element of the set of all least positive residues of $\{a, 2a, 3a, \ldots, (p-1)a\}$ which is equal to b_0. Hence there exists a unique $x \in \{1, 2, 3, \ldots, (p-1)\}$ such that $ax \equiv b_0 \equiv b \pmod{p}$. □

Theorem 13 (Chinese Remainder Theorem)**.** [13] *Suppose that $n_1, \ldots, n_k$ are k positive integers that are pairwise coprime. Then, for any given sequence of integers $a_1, \ldots, a_k$, there exists an integer x solving the following system of simultaneous congruence.*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad\vdots \\ x \equiv a_k \pmod{n_k} \end{cases}.$$

Furthermore, any two solutions of this system are congruent modulo $N = n_1 \cdots n_k$.

Proof. Let $S = \{0, 1, 2, \ldots, N-1\}$ and

$$T = \{(t_1, t_2, \ldots, t_k) | t_i \in \{0, 1, \ldots, n_i - 1\} \quad \text{for } i = 1, 2, \ldots, k\}.$$

Define $f : S \to T$ by $f(x) = (x_1, x_2, \ldots, x_k)$, where $x \equiv x_i \pmod{n_i}$ for $i = 1, 2, \ldots, k$.
If $x, y \in S$ and $f(x) = f(y) = (y_1, y_2, \ldots, y_k)$, then $x_i = y_i$ for $i = 1, 2, \ldots, k$. This implies that $x \equiv y \pmod{n_i}$ for $i = 1, 2, \ldots, k$.
$x - y$ is divisible by n_i for $i = 1, 2, \ldots, k$. Since $n_1, n_2, \ldots, n_k$ are pairwise coprime, $x - y$ is divisible by $N = n_1 \cdots n_k$. So $x = y$.
Note that $|S| = N = |T|$. f is a bijection.
For any $(a_1, a_2, \ldots, a_k) \in T$, there exist a unique x such that $f(x) = (a_1, a_2, \ldots, a_k)$.
For this x, $x \equiv a_i \pmod{n_k}$ for $i = 1, 2, \ldots, k$.
If $x'$is a solution of the simultaneous congruence, $x' - x$ is divisible by all of

$n_1, n_2, \ldots, n_k$ and hence is divisible by $N = n_1 \cdots n_k$.
Therefore, $x' \equiv x \,(\mathrm{mod}\, N)$ □

Theorem 14 ((Fermats Little Theorem)**.** [14] *Let p be a prime and a be an integer not divisible by p. Then $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$.*

Proof. By Theorem 11,

$$\begin{aligned} a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) && (\mathrm{mod}\, p) \\ (p-1)!a^{p-1} &\equiv (p-1)! && (\mathrm{mod}\, p) \end{aligned}$$

Since $(p-1)!$ is not divisible by p,

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$$

□

Theorem 15 (Wilsons Theorem)**.** [15] *Let p be prime. Then $(p-1)! \equiv 1 \,(\mathrm{mod}\, p)$.*

Proof. By Theorem 12, for any $a \in \{1, 2, 3, \ldots, (p-1)\}$, there exist a unique x in the set $\{1, 2, 3, \ldots, (p-1)\}$ such that $ax \equiv 1 \,(\mathrm{mod}\, p)$.
Note that $x = a$ if and only if $a^2 - 1 = (a+1)(a-1)$ is divisible by p. So 1 and $p-1$ are the only values of a such that $x = a$.
For other values of a, $a \neq x$. Therefore, the elements of $\{2, 3, 4, \ldots, p-2\}$ can be grouped into pairs of distinct a and x such that $ax \equiv 1 \,(\mathrm{mod}\, p)$. [See reviewer's comment (7)]
So

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1) \\ &\equiv 1 \cdot (p-1) && (\mathrm{mod}\, p) \\ &\equiv -1 && (\mathrm{mod}\, p) \end{aligned}$$

□

4.2. Quadratic residues

Definition 16 (Quadratic residue)**.** [16] *Let $n \geq 2$ be an integer. An integer q is called a quadratic residue of n if there exist an integer x such that $x^2 \equiv q \,(\mathrm{mod}\, n)$. Otherwise, q is called a quadratic nonresidue of n.*

Remark 17. *0 and 1 are quadratic residue of n for all $n \geq 2$.*

Theorem 18. *Let a be a quadratic residue of p, where p is an odd prime and a is not divisible by p. Then for any positive integer n, a is a quadratic residue of p^n.*

Proof. Let k be a positive integer. Suppose that $a \equiv x^2 \,(\mathrm{mod}\, p^k)$ for some integer x. Then $x^2 = tp^k + a$ for some integer t. So for any integer s,

$$(x + sp^k)^2 = x^2 + 2xsp^k + s^2p^{2k}$$

$$\begin{aligned} &= a + p^k(t + 2xs + s^2p^k) \\ &\equiv a + p^k(t + 2xs) \pmod{p^{k+1}} \end{aligned}$$

Since p is prime and $2x$ is not divisible by p, by Theorem 12, there exists an integer λ such that $(2x)(\lambda) \equiv 1 \pmod{p}$. Take $s = -\lambda t$. Then $t + 2xs = t - 2x\lambda t \equiv t - t \equiv 0 \pmod{p}$ and hence

$$(x + sp^k)^2 \equiv a + p^k(t + 2xs) \equiv a \pmod{p^{k+1}}.$$

a is a quadratic residue of p^{k+1}. By the principle of mathematical induction, a is a quadratic residue of p^n for all positive integers n. □

Remark 19. *Theorem 18 does not hold for $p = 2$. Note that 3 is a quadratic residue of 2 but is a quadratic nonresidue of 4.*

Theorem 20. *Let a be an odd integer which is a quadratic residue of 8. Then for all integers $n > 3$, a is a quadratic residue of 2^n.*

Proof. Let $k \geq 3$ be an integer. Suppose that $a \equiv x^2 \pmod{2^k}$ for some integer x. Then $x^2 = 2^k t + a$ for some integer t. So for any integer s,

$$\begin{aligned} (x + s \cdot 2^{k-1})^2 &= x^2 + 2^k xs + 2^{2k-2}s^2 \\ &= a + 2^k xs + s^2(2^{k+1})(2^{k-3}) \\ &= a + 2^k(t + xs) \pmod{2^{k+1}}. \end{aligned}$$

Note that x is odd. Take $s = \begin{cases} 0 & \text{if } t \text{ is even} \\ 1 & \text{if } t \text{ is odd} \end{cases}$. Then $t + xs$ is even and hence $2^k(t + xs) \equiv 0 \pmod{2^{k+1}}$. So $(x + s \cdot 2^{k-1})^2 \equiv a \pmod{2^{k+1}}$.
a is a quadratic residue of 2^{k+1}. By the principle of mathematical induction, a is a quadratic residue of 2^n for $n > 3$. □

Theorem 21. *Let γ be a non-zero integer, p be a prime and λ be a non-negative integer such that p^λ divides λ but $p^{\lambda+1}$ does not. Suppose that α is a non-negative integer.*

(1) *When λ is odd, γ is a quadratic residue of p^α if and only if $\alpha \leq \lambda$.*
(2) *When $p = 2$, λ is even and $\dfrac{\gamma}{2^\lambda} \equiv 3 \pmod{4}$, γ is a quadratic residue of p^α if and only if $\alpha \leq \lambda + 1$.*
(3) *When $p = 2$, λ is even and $\dfrac{\gamma}{2^\lambda} \equiv 5 \pmod{8}$, γ is a quadratic residue of p^α if and only if $\alpha \leq \lambda + 2$.*
(4) *When $p = 2$, λ is even and $\dfrac{\gamma}{2^\lambda} \equiv 1 \pmod{8}$, γ is a quadratic residue of p^α for any α.*
(5) *When $p > 2$, λ is even and $\dfrac{\gamma}{p^\lambda}$ is quadratic nonresidue of p, γ is a quadratic residue of p^α if and only if $\alpha \leq \lambda$.*

(6) *When $p > 2$, λ is even and $\dfrac{\gamma}{p^\lambda}$ is quadratic residue of p, γ is a quadratic residue of p^α for any α.*

Proof. When $\alpha \leq \lambda$, $\gamma \equiv 0 \equiv (0)^2 \pmod{p^\alpha}$ and hence γ is a quadratic residue of p^α.

Suppose that $x^2 \equiv \gamma \pmod{p^\alpha}$.
When λ is odd and $\alpha \geq \lambda + 1$, $x^2 \equiv \gamma \pmod{p^{\lambda+1}}$. Since x^2 is divisible by p^λ and λ is odd, x is divisible by $p^{\frac{\lambda+1}{2}}$. So we have

$$\gamma \equiv p^{\lambda+1} \left(\frac{x}{p^{\frac{\lambda+1}{2}}} \right)^2 \pmod{p^{\lambda+1}}$$

$$\frac{\gamma}{p^\lambda} \equiv p \left(\frac{x}{p^{\frac{\lambda+1}{2}}} \right)^2 \equiv 0 \pmod{p}$$

which is not true as $p^{\lambda+1}$ does not divide γ. This proves (1).
When λ is even and $\alpha \geq \lambda + 1$. Since x^2 is divisible by p^λ and λ is even, x is divisible by $p^{\frac{\lambda}{2}}$. So $\dfrac{x}{p^{\frac{\lambda}{2}}}$ is an integer and $p^\lambda \left(\dfrac{x}{p^{\frac{\lambda}{2}}} \right)^2 = x^2 \equiv \gamma \pmod{p^\alpha}$ is equivalent to $\left(\dfrac{x}{p^{\frac{\lambda}{2}}} \right)^2 \equiv \dfrac{\gamma}{p^\lambda} \pmod{p^{\alpha-\lambda}}$. γ is a quadratic residue of p^α if and only if $\dfrac{\gamma}{p^\lambda}$ is a quadratic residue of $p^{\alpha-\lambda}$.

Now suppose that $p = 2$. Note that $\dfrac{\gamma}{2^\lambda} \equiv 1 \equiv (1)^2 \pmod{2}$.
Since any perfect square is congruent to 0 or 1 modulo 4, if $\dfrac{\gamma}{2^\lambda} \equiv 3 \pmod{4}$, then $\dfrac{\gamma}{2^\lambda}$ is a quadratic nonresidue of 4 and therefore $\alpha - \lambda \leq 1$. This proves (2).

If $\dfrac{\gamma}{2^\lambda} \equiv 5 \pmod{8}$, them $\dfrac{\gamma}{2^\lambda} \equiv 1 \equiv (1)^2 \pmod{4}$.
Since 1^2, 3^2, 5^2 and 7^2 are all congruent to 1 modulo 8, 5 is a quadratic nonresidue of 8. So $\alpha - \lambda \leq 2$ and this proves (3).

If $\dfrac{\gamma}{2^\lambda} \equiv 1 \pmod{8}$, then $\dfrac{\gamma}{2^\lambda}$ is a quadratic residue of 8. By Theorem 20, $\dfrac{\gamma}{2^\lambda}$ is a quadratic residue of $2^{\alpha-\lambda}$ and thus λ is a quadratic residue of 2^α. This proves (4).

When $p > 2$, $\alpha \geq \lambda + 1$ and λ is even, γ is a quadratic residue of p^α if and only if $\dfrac{\gamma}{p^\lambda}$ is a quadratic residue of $p^{\alpha-\lambda}$.
By Theorem 18, if $\dfrac{\gamma}{p^\lambda}$ is a quadratic residue of p, then $\dfrac{\gamma}{p^\lambda}$ is a quadratic residue of $p^{\alpha-\lambda}$. The converse is obviously true.
This proves (5) and (6). □

Theorem 22 (Euler's Criterion)**.** [9] *Let p be an odd prime and a be an integer coprime to p. Then $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ if and only if a is a quadratic residue of p, and $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ if and only if a is a quadratic nonresidue of p.*

Proof. We will prove the theorem in three steps.

(1) $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ if a is a quadratic nonresidue of p.
(2) $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ if a is a quadratic residue of p.
(3) a is a quadratic residue of p if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ and a is a nonquadratic residue of p if $a^{\frac{p-1}{2}} \equiv -11 \pmod p$.

Suppose that a is a quadratic nonresidue of p. Let $b \in \{1, 2 \ldots, p1\}$. By Theorem 12, there exists a unique $b' \in \{1, 2, 3, \ldots, p1\}$ such that $b \cdots b' \equiv a \pmod p$. Note that $b' \neq b$, as otherwise, $b^2 \equiv a \pmod p$ and a will be a quadratic residue of p.
So the elements of $\{1, 2 \ldots, p1\}$ can be divided into pairs of distinct b, b' such that$b \cdots b' \equiv a \pmod p$.
Therefore

$$(p-1)! = 1 \cdots 2 \cdots 3 \ldots \cdots (p-1) \equiv a^{\frac{p-1}{2}} \pmod p.$$

By Wilsons Theorem (Theorem 15),

$$(p-1)! \equiv -1 \pmod p.$$

Therefore $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Now suppose that a is a quadratic residue of p. Then there exists an integer c such that $c^2 \equiv a \pmod p$. Let c_0 be the least positive residue of c modulo p. Then $c_0^2 \equiv c^2 \equiv a \pmod p$. Let $y(\neq c_0)$ be an integer such that $1 \leq y \leq p1$ and $y^2 \equiv a \pmod p$. Then, we have $c_0^2 - y^2 \equiv 0 \pmod p$ and thus $(c_0 + y(c_0 - y)$ is a multiple of p. So at least one among $c_0 + y$ and $c_0 - y$ is a multiple of p. As $1 \leq c_0$, $y \leq p - 1$, $c_0 - y$ cannot be a multiple of p. So $c_0 + y$ must be a multiple of p and thus $c_0 + y = p$. Note that $c_0 \neq p - c_0$ as$p$ is odd. Among $\{1, 2 \ldots, p-1\}$, there are exactly two integers c_0 and $p - c_0$ satisfying the congruence $x^2 \equiv a \pmod p$. The remaining $p - 3$ integers in the set$\{1, 2 \ldots, p-1\}$ form pairs of distinct b, b' such that $b \cdots b' \equiv a \pmod p$. [See revewer's comment (8)] Therefore

$$\begin{aligned}
(p-1)! &= 1 \cdots 2 \ldots \cdots c_0 \cdots \ldots \cdots (p-c_0) \cdots \ldots \cdots (p-1) \\
&\equiv a^{\frac{p-3}{2}} \cdots c_0 \cdots (p-c_0) && \pmod p \\
&\equiv a^{\frac{p-3}{2}} \cdots c_0 \cdots (-c_0) && \pmod p \\
&\equiv a^{\frac{p-3}{2}} \cdots (-s) && \pmod p \\
&\equiv -a^{\frac{p-1}{2}} && \pmod p.
\end{aligned}$$

By Wilsons Theorem (Theorem 15), $(p-1)! \equiv -1 (\mathrm{mod}\, p)$. So

$$-1 \equiv -a^{\frac{p-1}{2}} \pmod p$$

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

By Fermat's Little Theorem (Theorem 14), $a^{p-1}-1$ is divisible by p. As $a^{p-1}-1 = \left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)$, at least one among $a^{\frac{p-1}{2}}-1$ and $a^{\frac{p-1}{2}}+1$ is divisible by p. Therefore, $a^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod{p}$.
Suppose that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. If a is a quadratic nonresidue of p, then by (1), $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ and leads to a contradiction.
So a is a quadratic residue of p if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
Now suppose that$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. If a is a quadratic residue of p, then by (2), $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and leads to a contradiction. Therefore a is a nonquadratic residue of p if $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Definition 23 (Legendre Symbol)**.** [17] *Let p be an odd prime number and a be an integer. The Legendre symbol is a function of a and p defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \text{ and } a \text{ is not divisible by } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p \\ 0 & \text{if } a \text{ is divisible by } p \end{cases}$$

Remark 24. *Theorem 22 (Eulers Criterion) can be reformulated as* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. *Note that when a is divisible by p,* $\left(\frac{a}{p}\right) \equiv 0 \equiv a^{\frac{p-1}{2}} \pmod{p}$

Theorem 25. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.[18]

Proof. $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$ □

Theorem 26 (Gauss Lemma)**.** [10] *Let p be an odd prime and a be a positive integer coprime to p. Let $S = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$ and n be the number of elements of S whose least positive residue modulo p is greater than $\frac{p}{2}$. Then $\left(\frac{a}{p}\right) = (-1)^n$.*

Proof. By Theorem 11, the least positive residue of the elements of S are mutually different.
Let S' be the set of the least positive residue of the elements of S modulo p. We arrange S' in ascending order.
$S' = \{b_1, b_2, \ldots, b_m, c_1, c_2, \ldots, c_n\}$ where $b_m < \frac{p}{2} < c_1$ and $m+n = \frac{p-1}{2}$. Let S" $= \{b_1, b_2, \ldots, b_m, p-c_1, p-c_2, \ldots, p-c_n\}$.
Obviously, all elements of S" are positive and smaller than $\frac{p}{2}$. So

$S" \subset \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$.

We will prove that $S" = \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$.

By Theorem 11, $b_1, b_2, \ldots, b_m$ are mutually distinct and $c_1, c_2, \ldots, c_n$ are mutually distinct. If $b_i = o - c_j$ for some positive integers i, j, let $b_i = ra$ and $c_j = sa$, where $1 \leq r, s \leq \frac{p-1}{2}$. Then

$$(r+s)a = ra + sa = b_i + c_j = p.$$

This is impossible as $2 \leq r + s \leq p - 1$ and therefore $r + s$ cannot be a factor of p. So for any $i \in \{1, 2, 3, \ldots, m\}$ and $j \in \{1, 2, 3, \ldots, n\}$, $b_i \neq p - c_j$. $b_1, b_2, \ldots, b_m, p - c_1, p - c_2, \ldots, p - c_n$ are mutually distinct and so $|S" = m + n = \frac{p-1}{2}$. Therefore $S" = \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$.

Hence, we have

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2} = b_1 \cdot b_2 \cdot b_3 \cdot \ldots \cdot b_m \cdot (p - c_1) \cdot (p - c_2) \cdot \ldots \cdot (p - c_n)$$

$$\left(\frac{p-1}{2}\right)! \equiv b_1 \cdot b_2 \cdot b_3 \cdot \ldots \cdot b_m \cdot (-c_1) \cdot (-c_2) \cdot \ldots \cdot (-c_n) \pmod{p}$$

$$\equiv (-1)^n \cdot b_1 \cdot b_2 \cdot b_3 \cdot \ldots \cdot b_m \cdot c_1 \cdot c_2 \cdot \ldots \cdot c_n \pmod{p}$$

$$\equiv (-1)^n \cdot a \cdot 2a \cdot 3a \cdot \ldots \cdot \left(\frac{p-1}{2}a\right) \pmod{p}$$

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$$

As $\left(\frac{p-1}{2}\right)!$ is not divisible by p, $1 \equiv (-1)^n \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$. By Eulers Criterion (Theorem 22), $\left(\frac{a}{p}\right) = (-1)^n$. □

Theorem 27. *Let p, q be distinct odd primes and $R = \{2, 4, \ldots, p-1\}$. Then* $\left(\frac{q}{p}\right) = (-1)^{\sum\limits_{u \in R} \left\lfloor \frac{uq}{p} \right\rfloor}$. [See reviewer's comment (9)]

Proof. Let $S = \left\{q, 2q, 3q, \ldots, \frac{p-1}{2}q\right\}$ and n be the number of S whose least positive residue modulo p is greater that $\frac{p}{2}$. Then by Gauss Lemma (Theorem 26), $\left(\frac{q}{p}\right) = (-1)^n$.

If $u \in R$, then $\frac{uq}{2} \in S$. Let θ be the least positive residue of $\frac{uq}{2}$ modulo p. Then $\frac{uq}{2} = tp + \theta$ for some $t \in mathbfZ$. Note that $\theta \neq \frac{p}{2}$.

If $0 < \theta < \frac{p}{2}$, $\frac{uq}{p} = 2t + \frac{2\theta}{p} \in (2t, 2t+1)$ and hence $\left\lfloor \frac{uq}{p} \right\rfloor = 2t$.

If $\frac{p}{2} < \theta < p$, $\frac{uq}{p} = 2t + \frac{2\theta}{p} \in (2t+1, 2t+2)$ and hence $\left\lfloor \frac{uq}{p} \right\rfloor = 2t+1$.

Therefore, $\left\lfloor \frac{uq}{p} \right\rfloor$ is odd if and only if $\theta > \frac{p}{2}$.

$\sum_{u\in R} \left\lfloor \frac{uq}{p} \right\rfloor \equiv n \pmod 2$ and hence $\left(\frac{q}{p}\right) = (-1)^{\sum_{u\in R}\left\lfloor \frac{uq}{p} \right\rfloor}$. □

Theorem 28 (Law of Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.[18]

Proof. Let $R = \{2, 4, \ldots, p-1\}$, $R_1 = \left\{x \in R | x < \frac{p}{2}\right\}$, $T = 1, 3, \ldots, p-2$ and $T_1 = \left\{x \in T | x < \frac{p}{2}\right\}$.

Note that $u \in R \setminus R_1$ if and only if $p - u \in T_1$.

Therefore,

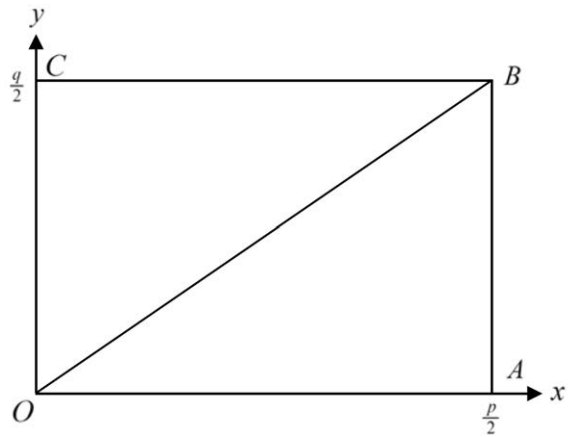
$$\sum_{u\in R\setminus R_1} \left\lfloor \frac{uq}{p} \right\rfloor = \sum_{u\in T_1} \left\lfloor \frac{(p-u)q}{p} \right\rfloor = \sum_{u\in T_1} \left\lfloor q - \frac{uq}{p} \right\rfloor = \sum_{u\in R} \left(q - 1 - \left\lfloor \frac{uq}{p} \right\rfloor\right)$$

and hence

$$\begin{aligned}
\sum_{u\in R} \left\lfloor \frac{uq}{p} \right\rfloor &= \sum_{u\in R_1} \left\lfloor \frac{uq}{p} \right\rfloor + \sum_{u\in R\setminus R_1} \left\lfloor \frac{uq}{p} \right\rfloor \\
&= \sum_{u\in R_1} \left\lfloor \frac{uq}{p} \right\rfloor + \sum_{u\in R} \left(q - 1 - \left\lfloor \frac{uq}{p} \right\rfloor\right) \\
&= \sum_{u\in R_1} \left\lfloor \frac{uq}{p} \right\rfloor + \sum_{u\in T_1} \left\lfloor \frac{uq}{p} \right\rfloor + \sum_{u\in R} \left(q - 1 - 2\left\lfloor \frac{uq}{p} \right\rfloor\right) \\
&= \sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{uq}{p} \right\rfloor + \sum_{u\in R} \left(q - 1 - 2\left\lfloor \frac{uq}{p} \right\rfloor\right).
\end{aligned}$$

Since $q-1$ is even, $\sum_{u\in R}\left\lfloor \frac{uq}{p}\right\rfloor \equiv \sum_{u=1}^{\frac{p-1}{2}}\left\lfloor \frac{uq}{p}\right\rfloor \pmod 2$.

By Theorem 27, $\left(\frac{q}{p}\right)=(-1)^{\sum_{u=1}^{\frac{p-1}{2}}\left\lfloor \frac{uq}{p}\right\rfloor}$.



Take four points $O(0,0)$, $A\left(\frac{p}{2},0\right)$, $B\left(\frac{p}{2},\frac{q}{2}\right)$ and $C\left(0,\frac{q}{2}\right)$ on a rectangular coordinate plane. The equation of the line segment OB is $y=\frac{q}{p}x$. Note that there is no lattice point on the line segment OB. For $u=1,2,\ldots,\frac{p-1}{2}$, $\left\lfloor \frac{uq}{p}\right\rfloor$ is the number of lattice points between the x-axis and the line OB with x-coordinate equals u. So, $\sum_{u=1}^{\frac{p-1}{2}}\left\lfloor \frac{uq}{p}\right\rfloor$ is equal to the number of lattice points in the interior of $\triangle OAB$.

By symmetry, $\left(\frac{p}{q}\right)=(-1)^{\sum_{u=1}^{\frac{q-1}{2}}\left\lfloor \frac{up}{q}\right\rfloor}$, and $\sum_{u=1}^{\frac{q-1}{2}}\left\lfloor \frac{up}{q}\right\rfloor$ is equal to the number of lattice points in the interior of $\triangle OBC$.

If σ is the number of lattice points in the interior of $OABC$, then

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)&=(-1)^{\sum_{u=1}^{\frac{q-1}{2}}\left\lfloor \frac{up}{q}\right\rfloor}(-1)^{\sum_{u=1}^{\frac{p-1}{2}}\left\lfloor \frac{uq}{p}\right\rfloor}\\&=(-1)^{\sum_{u=1}^{\frac{q-1}{2}}\left\lfloor \frac{up}{q}\right\rfloor+\sum_{u=1}^{\frac{p-1}{2}}\left\lfloor \frac{uq}{p}\right\rfloor}\\&=(-1)^{\sigma}\\&=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\end{aligned}$$

$$= (-1)^{\frac{(p-1)(q-1)}{4}}$$

□

Theorem 29 (First Supplement to the Law of Quadratic Reciprocity)**.** *Let p be a prime. -1 is a quadratic residue of p if and only if $p \equiv 1 \pmod 4$.* [18]

Proof. By By Eulers Criterion (Theorem 22), $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. So 1 is a quadratic residue of p if and only if $\frac{p-1}{2} \equiv 0 \pmod 2$, i.e. $p \equiv 1 \pmod 4$. □

Theorem 30 (Second Supplement to the Law of Quadratic Reciprocity)**.** [11] *Let p be an odd prime. 2 is a quadratic residue of p if and only if $p \equiv \pm 1 \pmod 8$.*

Proof. Let $S = \left\{2 \cdot 1, 2 \cdot 2, 2 \cdot 3, \ldots, 2 \cdot \frac{p-1}{2}\right\} = \{2, 4, 6, \ldots, p-1\}$.
Let n be the number of elements of S whose least positive residue modulo p is greater than $\frac{p}{2}$ and k be the number of elements of S whose least positive residue modulo p is smaller than $\frac{p}{2}$. As all elements of S are less that p, n is the number of elements of S which are greater than $\frac{p}{2}$. Since $2x \leq \frac{p}{2}$ if and only if $x \leq \frac{p}{4}$, $k = \left\lfloor \frac{p}{4} \right\rfloor$.
So $n = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$. There are four possible cases.

(1) $p = 8r + 1$, where r is some positive integer.
Then $n = \frac{8r+1-1}{2} - \left\lfloor \frac{8r+1}{4} \right\rfloor = 4r - 2r = 2r$.
(2) $p = 8r + 3$, where r is some positive integer.
Then $n = \frac{8r+3-1}{2} - \left\lfloor \frac{8r+3}{4} \right\rfloor = 4r + 1 - 2r = 2r + 1$.
(3) $p = 8r + 5$, where r is some positive integer.
Then $n = \frac{8r+5-1}{2} - \left\lfloor \frac{8r+5}{4} \right\rfloor = 4r + 2 - (2r + 1) = 2r + 1$.
(4) $p = 8r + 7$, where r is some positive integer.
Then $n = \frac{8r+7-1}{2} - \left\lfloor \frac{8r+7}{4} \right\rfloor = 4r + 3 - (2r + 1) = 2r + 2$.

So n is even when $p \equiv \pm 1 \pmod 8$.
By Gauss Lemma (Theorem 26), 2 is a quadratic residue of p if and only if n is even, i.e. $p \equiv \pm 1 \pmod 8$. □

Theorem 31. *Suppose $n_1, n_2, \ldots, n_k$ are positive integers that are pairwise co-prime, and a is a quadratic residue of n_j for all $j = 1, 2, \ldots, k$. Then a is a quadratic residue of $n_1 n_2 \cdots n_k$.*

Proof. Let $x_1, x_2, \ldots, x_k$ be integers such that $x_i^2 \equiv a \pmod{n_j}$ for $j = 1, 2, \ldots, k$. By Chinese Remainder Theorem (Theorem 13), there exists an integer x such that $x \equiv x_j \pmod{n_j}$ for all $j = 1, 2, \ldots, k$. So for all j, $x^2 \equiv x_i^2 \equiv a \pmod{n_j}$. Therefore, $x^2 - a$ is divisible by all of $n_1, n_2, \ldots, n_k$. As $n_1, n_2, \ldots, n_k$ are pairwise coprime, $x^2 - a$ is divisible by $n_1 n_2 \cdots n_k$. So a is a quadratic residue of $n_1 n_2 \cdots n_k$. □

4.3. When $a^2 + 2$ is the sum of two squares

Theorem 32. *Let $l > 1$ be an odd integer. 2 is a quadratic residue of l if and only if there exist integers a and b such that $a^2 + 2 = (a - l)^2 + b^2$.*

Proof. Suppose there exist integers a and b such that $a^2 + 2 = (a - l)^2 + b^2$. Then

$$b^2 = a^2 - (a - l)^2 + 2 = 2al - l^2 + 2 \equiv 2 \pmod{l}$$

So 2 is a quadratic residue of l.
Conversely, suppose that 2 is a quadratic residue of l. Let x be an integer such that $1 \leq x < l$ and $x^2 \equiv 2 \pmod{l}$. Then $x^2 = lt + 2$ for some integer t.
If t is odd, let $a = \dfrac{l + t}{2}$. Then a is an integer and

$$a^2 + 2 - (a - l)^2 = l(2a - l) + 2 = lt + 2 = x^2.$$

Take $b = x$ and we have $a^2 + 2 = (a - l)^2 + b^2$.
If t is even, let $a = l + x + \dfrac{t}{2}$. Then a is an integer and

$$\begin{aligned} a^2 + 2 - (a - l)^2 &= l(2a - l) + 2 = lt + 2 = x^2 \\ &= l(l + 2x + t) + 2 \\ &= l^2 + 2lx + x^2 \\ &= (l + x)^2 \end{aligned}$$

Take $b = l + x$ and we have $a^2 + 2 = (a - l)^2 + b^2$. □

Theorem 33. *Let $l > 1$ be an integer. There exist integers a and b such that $a^2 + 2 = (a - l)^2 + b^2$ if and only if all prime factors of l are in the form of $8k \pm 1$.*

Proof. Suppose there exist integers a and b such that $a^2 + 2 = (a - l)^2 + b^2$.
If l is even, $a^2 - (a - l)^2 + 2 = 2al - l^2 + 2 \equiv 2 \pmod{4}$ and cannot be a perfect square. So l is an odd integer.
$b^2 - 2 = 2al - l^2$ is divisible by l and hence is divisible by p. Therefore, 2 is a quadratic residue of p. By the Second Supplement to the Law of Quadratic Reciprocity (Theorem 30), $p \equiv \pm 1 \pmod{8}$.
Any prime factor of l is in the form of $8k \pm 1$.
Conversely, suppose that $l = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$, where $p_1, p_2, \ldots, p_n$ are mutually distinct odd primes, all in the form of $8k \pm 1$, and $k_1, k_2, \ldots, k_n$ are positive integers. By the Second Supplement to the Law of Quadratic Reciprocity (Theorem 30), 2

is a quadratic residue of p_i for $i = 1, 2, \ldots, n$. So Theorem 18 implies that 2 is a quadratic residue of $l = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$. By Theorem 32 ,there exist integers a and b such that $a^2 + 2 = (a - l)^2 + b^2$. □

5. Begin with squares

With the results of Chapter 4, we can now construct $1, 2$-triples beginning with perfect squares. We will first find the square roots of 2 modulo l for those values of l satisfying the condition stated in Theorem 33. Then we can give the general form of such kind of $1, 2$-triples corresponding to l.

5.1. Square roots of 2 modulo p^k

As shown in the proof of Eulers Criterion (Theorem 22), $x^2 \equiv 2 \pmod{p}$ have exactly two distinct solutions for $1 \leq x \leq p-1$, and the sum of these two solutions is p. As $p - x \equiv -x \pmod{p}$, the square roots of 2 modulo p can be written as $\pm x$. The square roots of 2 modulo p for the first few prime p of the form $n \pm 18$ are listed in TABLE 7.

p	7	17	23	31	41	47	71	73	79	89
square roots of 2	± 3	± 6	± 5	± 8	± 17	± 7	± 12	± 32	± 9	± 25

TABLE 7. The square roots of 2 modulo p

When we have the square roots of 2 modulo p, square roots of 2 modulo p^2 can be found by the following method. Take $p^2 = 7^2 = 49$ as an example.
If $x^2 \equiv 2 \pmod{49}$, then $x^2 \equiv 2 \pmod{7}$. As shown in TABLE 7, $x = 7n \pm 3$ for some integer n. Therefore $(7n \pm 3) \overset{\equiv}{} 2 \pmod{49}$.

$$\begin{aligned} 49n^2 \pm 42n + 9 &\equiv 2 && \pmod{49} \\ \pm 42n &\equiv -7 && \pmod{49} \\ \pm 6n &\equiv -1 && \pmod{7} \end{aligned}$$

By Theorem 12, both $6n \equiv -1 \pmod{7}$ and $-6n \equiv -1 \pmod{7}$ have unique solutions modulo 7.
When $6n \equiv -1 \pmod{7}$, $n \equiv 1 \pmod{7}$.
When $-6n \equiv -1 \pmod{7}$, $n \equiv -1 \pmod{7}$.
The square of 2 modulo 49 are therefore ± 10.
The case for higher powers of p is similar.
[See reviewer's comment (10)]
If $x^2 \equiv 2 \pmod{p^{m+1}}$, $x^2 \equiv 2 \pmod{p^m}$. So $x = p^m n + k$ for some integers n and k such that $k^2 \equiv 2 \pmod{p^m}$.

$$(p^m n + k)^2 \equiv 2 \qquad \pmod{p^{m+1}}$$

p	7	17	23	31	41	47
square roots of 2 modulo p	± 3	± 6	± 5	± 8	± 17	± 7
square roots of 2 modulo p^2	± 10	± 45	± 156	± 116	± 58	± 477
square roots of 2 modulo p^3	± 108	± 623	± 156	± 2767	± 20230	± 8359

TABLE 8. The square roots of 2 modulo p^m

$$\begin{aligned} p^{2m}n^2 = 2p^m nk + k^2 &\equiv 2 && (\mathrm{mod}\, p^{m+1}) \\ 2p^m nk &\equiv 2 - k^2 && (\mathrm{mod}\, p^{m+1}) \\ (2k)n &\equiv \frac{2-k^2}{p^m} && (\mathrm{mod}\, p) \end{aligned}$$

Since $\dfrac{2-k^2}{p^m}$ is an integer, by Theorem 12, there exists a unique n modulo p satisfying the linear congruence $(2k)n \equiv \dfrac{2-k^2}{p^m} \,(\mathrm{mod}\, p)$. Given all the square roots of 2 modulo p^m, we can find all square roots of 2 modulo p^{m+1}.

5.2. Square roots of 2 modulo l

Let $1 > l$ be an odd integer such that all prime factors of l are in the form of $8k \pm 1$. By Theorem 30 (Second Supplement to the Law of Quadratic Reciprocity) and Theorem 31, the square roots of 2 modulo l exist.

Example 34. *Let* $l = 7 \cdot 17 = 119$. *As shown un TABLE 7,* $(\pm 3)^2 \equiv 2 \,(\mathrm{mod}\, 7)$ *and* $(\pm 6)^2 \equiv 2 \,(\mathrm{mod}\, 17)$. *By Chinese Remainder Theorem (Theorem 13), four square roots of* 2 *modulo* 119 *can be found. We will first focus on the case combining* $x \equiv 3 \,(\mathrm{mod}\, 7)$ *and* $x \equiv 6 \,(\mathrm{mod}\, 17)$.
Note that $5 \cdot 17 \equiv 1 \,(\mathrm{mod}\, 7)$ *and* $5 \cdot 7 \equiv 1 \,(\mathrm{mod}\, 17)$.
Let $y = 3 \cdot 5 \cdot 17 + 6 \cdot 5 \cdot 7 = 465 \equiv -11 \,(\mathrm{mod}\, 119)$.
Then $y = 3 \cdot 5 \cdot 17 \equiv 3 \cdot 1 \equiv 3 \,(\mathrm{mod}\, 7)$ *and* $y = 6 \cdot 5 \cdot 7 \equiv 6 \cdot 1 \equiv 6 \,(\mathrm{mod}\, 17)$.
Thus -11 *is a solution to the simultaneous congruence and hence is a square root of* 2 *modulo* 119.
By using this method in all cases, the square roots of 2 *modulo* 119 *are* ± 11 *and* ± 45.

Example 35. *Let* $l = 7 \cdot 17 \cdot 23^2 = 62951$. *As* l *has three distinct prime factors od the form* $8k \pm 1$, *there are totally* 8 *square roots of* 2 *modulo* l. *By Example 34 and TABLE 8,* $) \pm 11)^2 \equiv 2 \,(\mathrm{mod}\, 119)$, $(\pm 45)^2 \equiv 2 \,(\mathrm{mod}\, 119)$ *and* $(\pm 156)^2 \equiv 2 \,(\mathrm{mod}\, 23^2)$.
Note that $9 \cdot 23^2 \equiv 1 \,(\mathrm{mod}\, 119)$ *and* $489 \cdot 119 \equiv 1 \,(\mathrm{mod}\, 23^2)$.

t	(a, b)	$1,2$-triples
0	$(4, \pm 3)$	$(16, 17, 18)$
1	$(12, 11)$, $(24, 17)$	$(144, 145, 146)$, $(576, 577, 578)$
2	$(48, 25)$, $(72, 31)$	$(2304, 2305, 2306)$, $(5184, 5185, 5186)$
3	$(112, 39)$, $(148, 45)$	$(12544, 12545, 12546)$, $(21904, 21905, 21906)$

TABLE 9. $1,2$-triples (a^2, a^2+1, a^2+2) with $a = 14t^2 \pm 6t + 4$

Let $y = 11 \cdot 9 \cdot 23^2 + 156 \cdot 489 \cdot 119 = 9130167 \equiv 2272 \pmod{62951}$. *Then*

$$y \equiv 11 \cdot 9 \cdot 529 \equiv 11 \cdot 1 \equiv 11 \pmod{119}$$

and

$$y = 156 \cdot 489 \cdot 119 \equiv 156 \cdot 1 \equiv 156 \pmod{529}$$

Thus 2272 *is a solution to the simultaneous congruence and hence is a square root of* 2 *modulo* 62951. *By using this method in all cases, the square roots of* 2 *modulo* 62951 *are* ± 2272, ± 12540, ± 23432 *and* ± 24707.

5.3. Sequence of $1,2$-triples

Knowing the square roots of 2 modulo l, we can find a formula generating $1,2$-triples. We first start with the case $l = 7$. Considering $a^2 + 2 = (a-7)^2 + b^2$,

$$\begin{aligned} a^2 + 2 &= 2^2 - 14a + 49 + b^2 \\ 14a - 49 &= b^2 - 2 \end{aligned}$$

So $b^2 \equiv 2 \pmod{7}$. As the square roots of 2 modulo 7 are ± 3, let $b = 7n \pm 3$. Then

$$\begin{aligned} 14a - 49 &= (7n \pm 3)^2 - 2 \\ 49n^2 &\pm 42n + 7 \\ 2a &= 7n^2 \pm 6n + 8 \end{aligned}$$

Since both $2a$ and $\pm 6n + 8$ are even, n^2 is even and so is n.
Let $n = 2t$. Then

$$\begin{aligned} 2a &= 7(2t)^2 \pm 6(2t) + 8 \\ a &= 14t^2 \pm 6t + 4 \end{aligned}$$

(a^2, a^2+1, a^2+2) is an 1,2-triple and $a^2 + 2 = (14t^2 \pm 6t - 3)^2 + (14t \pm 3)^2$. Note that this gives the general formula for the $1,2$-triples of form (a^2, a^2+1, a^2+2) with $a^2 + 2 = (a-7)^2 + b^2$ for some integer b.

5.4. $1, 2$-triples beginning with perfect squares

For general $1 > l$ such that all prime factors of l are in the form of $8k \pm 1$, the corresponding $1, 2$-triples of form $(a^2, a^2 + 1, a^2 + 2)$ can be found if we know the square roots of 2 modulo l.

Let $a^2 + 2 = (a - l)^2 + b^2$. Then

$$a^2 + 2 = a^2 - 2al + l^2 + b^2$$
$$2al - l^2 = b^2 - 2$$

We have $b^2 \equiv 2 \pmod{l}$[13].
Let $\theta^2 \equiv 2 \pmod{l}$ and $b = nl + \theta$ for some integer n. Then

$$2al - l^2 = (nl + \theta)^2 - 2 = n^2l^2 + 2nl\theta + \theta^2 - 2$$

Since $\theta^2 \equiv 2 \pmod{l}$, $\dfrac{\theta^2 - 2}{l}$ is an integer.
Therefore,

$$2a - l = n^2l + 2n\theta + \frac{\theta^2 - 2}{l}$$
$$2a = (n^2 + 1)l + 2n\theta + \frac{\theta^2 - 2}{l}$$

If $\dfrac{\theta^2 - 2}{l}$ is odd, n^2 is even and son is n. [See reviewer's comment (11)] Let $n = 2t$. Then,

$$2a = ((2t)^2 + 1)l + 2(2t)\theta + \frac{\theta^2 - 2}{l}$$
$$a = 2lt^2 + 2t\theta + \frac{\theta^2 - 2}{2l} + \frac{l}{2}$$

$(a^2, a^2 + 1, a^2 + 2)$ is an $1, 2$-triples and

$$a^2 + 2 = \left(2lt^2 + 2t\theta + \frac{\theta^2 - 2}{2l} + \frac{l}{2}\right)^2 + (2lt + \theta)^2.$$

Note that if $\dfrac{\theta^2 - 2}{l}$ is even, $\dfrac{(\theta - l)^2 - 2}{l} = \dfrac{l^2 - 2l\theta + \theta^2 - 2}{l} = l - 2\theta + \dfrac{\theta^2 - 2}{l}$ is odd. [See reviewer's comment (12)] As $\theta \equiv \theta - l \pmod{l}$, we can always replace a square root of 2 modulo l with a θ_0 congruence to that root modulo l so that $\dfrac{\theta_0^2 - 2}{l}$ is odd.

---

[13] In the case when $l = 1$, we have $b^2 = 2a + 1$ and hence b is an odd integer. $(a, b) = (2t^2 + 2t, 2t + 1)$ for some integer t.

l	(a, b)
1	$(2t^2 \pm 2t, 2t \pm 1)$
7	$(14t^2 \pm 6t + 4, 14t \pm 3)$
17	$(34t^2 \pm 22t + 12, 34t \pm 11)$
119	$(238t^2 \pm 22t + 60, 238t \pm 11)$, $(238t^2 \pm 90t + 68, 238t \pm 45)$
62951	$(125902t^2 \pm 49414t + 36324, 125902t \pm 24707)$, $(125902t^2 \pm 79038t + 43880, 125902t \pm 39519)$, $(125902t^2 \pm 100822t + 51660, 125902t \pm 50411)$, $(125902t^2 \pm 121358t + 60720, 125902t \pm 60679)$

TABLE 10. Solutions of $a^2 + 2 = (a - l)^2 + b^2$ for some values of l

6. Littlewood's Problem

6.1. Quadratic residues

It was shown in Chapter 5 that if 2 is a quadratic residue of l, then we can find all integers a such that $a^2 + 2 = (a - l)^2 + b^2$ for some integers b. Similarly, we can give solutions to $a^2 + k = (a - l)^2 + b^2$ if k is a quadratic residue of l. So it is natural to ask a question: Given an integer k, for what integer l is k a quadratic residue of l?

Example 36. [See reviewer's comment (13)] *Find all odd primes p such that* $\left(\frac{3}{p}\right) = 1$.

By the Law of Quadratic of Reciprocity (Theorem 28),
$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(3-1)(p-1)}{4}} = (-1)^{\frac{p-1}{2}}$.
If $p \equiv 1 \pmod 3$, $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$ *and therefore* $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$.
So in this case, $\left(\frac{3}{p}\right) = 1$ *if and only if* $\frac{p-1}{2}$ *is even, i.e.* $p \equiv 1 \pmod 4$.
By the Second Supplement to the Law of Quadratic Reciprocity (Theorem 30),
$\left(\frac{2}{3}\right) = -1$.
If $p \equiv -1 \pmod 3$, $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$ *and therefore* $\left(\frac{3}{p}\right) = -(-1)^{\frac{p-1}{2}}$.
So in this case, $\left(\frac{3}{p}\right) = 1$ *if and only if* $\frac{p-1}{2}$ *is odd, i.e.* $p \equiv -1 \pmod 4$.

Therefore, $\left(\frac{3}{p}\right) = 1$ *if and only if* $\begin{cases} p \equiv 1 \pmod 3 \\ p \equiv 1 \pmod 4 \end{cases}$ *or* $\begin{cases} p \equiv -1 \pmod 3 \\ p \equiv -1 \pmod 4 \end{cases}$, *i.e.* $p \equiv \pm 1 \pmod{12}$. *[See reviewer's comment (14)]*

Example 37. *Find all odd primes* p *such that* $\left(\frac{5}{p}\right) = 1$.

By the Law of Quadratic of Reciprocity (Theorem 28),
$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{(5-1)(p-1)}{4}} = 1$ *for all odd prime* p. *So we have* $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$.
If $p \equiv 1 \pmod 5$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$.
If $p \equiv -1 \pmod 5$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1$.
If $p \equiv 2 \pmod 5$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$.[14]
If $p \equiv -2 \pmod 5$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$.
Therefore, $\left(\frac{5}{p}\right) = 1$ *if and only if* $p \equiv \pm 1 \pmod 5$.

Example 38. *Find all odd primes* p *such that* $\left(\frac{6}{p}\right) = 1$. *Note that* $\left(\frac{6}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{2}{p}\right)$. $\left(\frac{6}{p}\right) = 1$ *if and only if* $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right)$.
If $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right) = 1$, $\begin{cases} p \equiv \pm 1 \pmod{12} \\ p \equiv \pm 1 \pmod 8 \end{cases}$ *and therefore* $p \equiv \pm 1 \pmod{24}$.
If $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right) = -1$, $\begin{cases} p \equiv \pm 5 \pmod{12} \\ p \equiv \pm 5 \pmod 8 \end{cases}$ *and therefore* $p \equiv \pm 5 \pmod{24}$.
$\left(\frac{6}{p}\right) = 1$ *if and only if* $p \equiv \pm 1$ *or* $\pm 5 \pmod{24}$. *[See reviewer's comment (15)]*

a	$\left(\frac{a}{p}\right) = 1$ if and only if	a	$\left(\frac{a}{p}\right) = 1$ if and only if
1	p is any prime	-1	$p \equiv 1 \pmod 4$
2	$p \equiv \pm 1 \pmod 8$	-2	$p \equiv 1, 3 \pmod 8$
3	$p \equiv \pm 1 \pmod{13}$	-3	$p \equiv 1 \pmod 3$
4	p is any prime	-4	$p \equiv 1 \pmod 4$

[14]It is due to the Second Supplement to the Law of Quadratic Reciprocity (Theorem 30).

5	$p \equiv \pm 1 \pmod 5$	-5	$p \equiv 1, 3, 7, 9 \pmod{20}$
6	$p \equiv \pm 1, \pm 5 \pmod{24}$	-6	$p \equiv 1, 5, 7, 11 \pmod{24}$
7	$p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$	-7	$p \equiv 1, 2, 4 \pmod 7$
8	$p \equiv \pm 1 \pmod 8$	-8	$p \equiv 1, 3 \pmod 8$
9	p is any prime	-9	$p \equiv 1 \pmod 4$
10	$p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$	-10	$p \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}$
11	$p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \pmod{44}$	-11	$p \equiv 1, 3, 4, 5, 9 \pmod{11}$
12	$p \equiv \pm 1 \pmod{12}$	-12	$p \equiv 1 \pmod 3$

TABLE 11. Conditions that a is a quadratic residue of p (odd prime not dividing a) [16]

6.2. Littlewoods Problem

J. E. Littlewood has raised the question of whether for given unequal positive numbers h, k there exist infinitely many numbers n for which n, $n+h$, $n+k$ are all sums of two squares.[4][15] This is equivalent to ask whether there exists infinitely many h, k-triples.
Obviously, the answer to Littlewoods Problem is affirmative when both h and k are perfect squares, as n, $n+h$, $n+k$ are all sums of two squares when n itself is a perfect square. The 2000 Putnam Problem is the special case when $h = 1$ and $k = 2$.

Note that if $(a, b, c) = (a, a+h, a+k)$, then $(a, c, b) = (a, a+k, a+h)$, $(b, a, c) = (b, b+(-h), b+(k-h))$, $(b, c, a) = (b, b+(k-h), b+(-h))$, $(c, a, b) = (c, c+(-k), c+(h-k))$ and $(c, b, a) = (c, c+(h-k), c+(-k))$.
So if there are infinitely many h, k-triples, there are infinitely many k, h-triples, $(-h), (k-h)$-triples, etc.
By the method used in Chapter 5, we can show that if at least one among $|h|, |k|, |h-k|$ is a perfect square, then there exist infinitely many h, k-triples.
[See reviewer's comment (16)] Without loss of generality, let $h = \lambda^2$. Let $n = a^2$. Then $n + h = a^2 + \lambda^2$.
Consider $a^2 + k = (a - l)^2 + b^2$.

$$b^2 = 2al - l^2 + k \equiv k \pmod l$$

[15]This was solved in 1973 by C. Hooley. [4]

If there is a pair of b and l satisfying the above quadratic congruence, we can generate infinitely many sets of h,k-triples using a method which is similar to that used in Chapter 5. [See reviewer's comment (17)]

Example 39. *Prove that there are infinitely many* $4,5$*-triples. Find all* $4,5$*-triples of the form* (a^2, a^2+4, a^2+5).

We need $b^2 \equiv 5 \pmod{l}$.
For example, $6^2 \equiv 5 \pmod{31}$. *The pair* $(b,l) = (6,31)$ *generates the* $4,5$*-triples*

$$\left((62t^2 \pm 12t + 16)^2, (62t^2 \pm 12t + 16)^2 + 4, (62t^2 \pm 12t + 16)^2 + 5\right).$$

Here $(62t^2 \pm 12t + 16)^2 + 4 = (62t^2 \pm 12t + 16)^2 + 2^2$ *and*

$$(62t^2 \pm 12t + 16)^2 + 5 = (62t^2 \pm 12t - 15)^2 + (62t + 6)^2.$$

This proves that there are infinitely many $4,5$*-triples.*
In general, a $4,5$*-triples with* n *being a perfect square has the form*[16]

$$\left(\left(\frac{lt^2}{2} + t\theta + \frac{\theta^2-5}{2l} + \frac{l}{2}\right)^2, \left(\frac{lt^2}{2} + t\theta + \frac{\theta^2-5}{2l} + \frac{l}{2}\right)^2 + 4, \left(\frac{lt^2}{2} + t\theta + \frac{\theta^2-5}{2l} + \frac{l}{2}\right)^2 + 5\right).$$

Note that $(1)^2 \equiv 5 \pmod{4}$, $(0)^2 \equiv 5 \pmod{5}$ *but* 5 *is neither a quadratic residue of* 8 *nor a quadratic residue of* 25. *By Example 37, for odd prime* p *other than* 5, $\left(\frac{5}{p}\right) = 1$ *if and only if* $p \pm 1 \pmod{5}$. *By Theorem 18 and Theorem 31.* 5 *is a quadratic residue of* l *if and if* $l = 2^\lambda 5^\mu \beta$, *where* $\lambda \in \{0,1,2\}$, $\mu \in \{0,1\}$ *and all prime factor of* β *are of the form* $5n \pm 1$. *But if* $\lambda = 2$, *then* l *is divisible by* 4 *and* $a^2 + 5 - (a-l)^2 = 2al - l^2 \equiv 5 \pmod{8}$, *and cannot be a perfect square.*
If $l = 2\beta$ *and* $\theta^2 \equiv 5 \pmod{l}$, *then* θ *is odd and hence* $\theta^2 - 5$ *is divisible by* 4. *Note that* $\theta^2 - 5$ *is also divisible by* $l = 2\beta$. *So* $\theta^2 - 5$ *is divisible* $2l = 4\beta$. *Thus* $\frac{lt^2}{2} + t\theta + \frac{theta^2-5}{2l} + \frac{l}{2}$ *is an integer for all integers* t.
If $l = \beta$ *and* $\theta^2 \equiv 5 \pmod{l}$, *then* $\frac{\theta^2-5}{l}$ *is an integer. If furthermore* $\frac{\theta^2-5}{l}$ *is odd, then* $\frac{lt^2}{2} + t\theta + \frac{\theta^2-5}{2l} + \frac{l}{2}$ *is an integer for all even integers* t. *If* $\frac{\theta^2-5}{l}$ *is even, then* $\frac{(\theta-l)^2-5}{l} = \frac{\theta^2-5}{l} - 2\theta + l$ *is odd. Since* $\theta \equiv \theta - l \pmod{l}$, *we can replace* θ *by* $\theta - l$. *So we can assume that* $\frac{\theta^2-5}{2l} + \frac{l}{2}$ *is an integer. We have*

$$\begin{aligned}\left(\frac{lt^2}{2} + t\theta + \frac{\theta^2-5}{2l} + \frac{l}{2}\right)^2 + 5 &= \left(\frac{lt^2}{2} + t\theta + \frac{\theta^2-5}{2l} - \frac{l}{2}\right)^2 \\ &\quad + 4\left(\frac{lt^2}{2} + t\theta + \frac{\theta^2-5}{2l}\right)\left(\frac{l}{2}\right) + 5 \\ &= \left(\frac{lt^2}{2} + t\theta + \frac{\theta^2-5}{2l} - \frac{l}{2}\right)^2 + l^2t^2 + 2lt\theta + \theta^2\end{aligned}$$

[16] If 1=l, we can generate the solution $(a,b) = (2t^2-2, 2t)$.

$$
\begin{aligned}
&- 5 + 5 \\
&= \left(\frac{lt^2}{2} + t\theta + \frac{\theta^2 - 5}{2l} - \frac{l}{2}\right)^2 + (lt + \theta)^2
\end{aligned}
$$

So $\left(\dfrac{lt^2}{2} + t\theta + \dfrac{\theta^2 - 5}{2l} + \dfrac{l}{2}\right)^2$ *starts a* $4, 5$*-triple if it is an integer.*

Example 40. *Find all* $6, 9$*-triples of the form* $(a^2, a^2 + 6, a^2 + 9)$.

We need $b^2 \equiv 6 \pmod{l}$.

By Example 38, for odd prime p *other than* 3, $\left(\dfrac{6}{p}\right) = 1$ *if and only if* $p \equiv \pm 1, \pm 5 \pmod{24}$. *By Theorem 21 and Theorem 31,* 6 *is a quadratic residue of* l *if and only if* $l = 2^\lambda 3^\mu \beta$ *where* $\lambda, \mu \in \{0, 1\}$ *and all prime factors of* β *are congruent to* ± 1 *or* ± 5 *modulo* 24.

If $\lambda = 1$, *then* l *is even and* $a^2 + 6 - (a - l)^2 = 2al - l^2 + 6 \equiv 2 \pmod{4}$, *and cannot be a perfect square. Therefore,* $\lambda = 0$ *and hence* l *is odd.*

If $\theta^2 \equiv 6 \pmod{l}$, *then* $\dfrac{\theta^2 - 6}{l}$ *is an integer. If furthermore* $\dfrac{\theta^2 - 6}{l}$ *is odd,* $\dfrac{\theta^2 - 6}{2l} + \dfrac{l}{2}$ *is an integer. If* $\dfrac{\theta^2 - 6}{l}$ *is even, then* $\dfrac{(\theta - l)^2 - 6}{l} = \dfrac{\theta - 6}{l} - 2\theta + l$ *is odd. Since* $\theta \equiv \theta - l \pmod{l}$., *we can replace* θ *by* $\theta - l$. *So we can always assume that* $\dfrac{\theta^2 - 6}{2l} + \dfrac{l}{2}$ *is an integer. We have*

$$
\begin{aligned}
\left(2lt^2 + 2t\theta + \frac{\theta^2 - 6}{2l} + \frac{l}{2}\right)^2 + 6 &= \left(2lt^2 + 2t\theta + \frac{\theta^2 - 6}{2l} - \frac{l}{2}\right)^2 \\
&\quad + 4\left(2lt^2 + 2t\theta + \frac{\theta^2 - 6}{2l}\right)\left(\frac{l}{2}\right) + 6 \\
&= \left(2lt^2 + 2t\theta + \frac{\theta^2 - 6}{2l} - \frac{l}{2}\right)^2 + 4l^2t^2 + 4lt\theta + \theta^2 \\
&\quad - 6 + 6 \\
&= \left(2lt^2 + 2t\theta + \frac{\theta^2 - 6}{2l} - \frac{l}{2}\right)^2 + (2lt + \theta)^2
\end{aligned}
$$

So $\left(2lt^2 + 2t\theta + \dfrac{\theta^2 - 6}{2l} + \dfrac{l}{2}\right)^2$ *starts a* $6, 9$*-triple.*

Note that $\left(2lt^2 + 2t\theta + \dfrac{\theta^2 - 6}{2l} + \dfrac{l}{2}\right)^2 + 9 = \left(2lt^2 + 2t\theta + \dfrac{\theta^2 - 6}{2l} + \dfrac{l}{2}\right)^2 + 3^2$.

In general, a $6, 9$*-triple starting with a perfect square has the form*[17]

$$\left(\left(2lt^2 + 2t\theta + \frac{\theta^2 - 6}{2l} + \frac{l}{2}\right)^2, \left(2lt^2 + 2t\theta + \frac{\theta^2 - 6}{2l} + \frac{l}{2}\right)^2 + 6, \left(2lt^2 + 2t\theta + \frac{\theta^2 - 6}{2l} + \frac{l}{2}\right)^2 + 9\right)$$

[17] If $l = 1$, we can generate the solution $(a, b) = (2t^2 - 2t - 2, 2t - 1)$.

6.3. Possible values of l

The key to solve $a^2 + k = (a - l)^2 + b^2$ is to find all possible values of l such that k is a quadratic residue of l.[18] With the help of Theorem 31, we can do it by first finding all possible prime powers that can be a factor of l. [See reviewer's comment (18)]
Denote the i-th prime by p_i (so $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ...). Suppose that $k = \prod p_i^{\lambda_i}$, where λ_i's are non-negative integers. Let $k_i = \prod_{i \neq j} p_i^{\lambda_i}$.

If $a^2 + k = (a - 2^{\alpha_1})^2 + b^2$, then $b^2 = a^2 - (a - 2^{\alpha_1})^2 + k = 2^{\alpha_1+1}a - 2^{2\alpha_1} + k$. So if $\alpha_1 \geq 1$, k is a quadratic residue of 2^{α_1+1}. By Theorem 21, when λ_1 is odd, k is a quadratic residue of 2^{α_1+1} if and only if $\alpha_1 \leq \lambda_1 - 1$. If λ_1 is even, then the highest power of 2 as a factor depends on both λ_1 and k_1. When λ_1 is even and $k_1 \equiv 3 \pmod 4$, k is a quadratic residue of 2^{α_1+1} if and only if $\alpha_1 \leq \lambda_1$. When λ_1 is even and $k_1 \equiv 5 \pmod 8$, k is a quadratic residue of 2^{α_1+1} if and only if $\alpha_1 \leq \lambda_1 + 1$. When λ_1 is even and $k_1 \equiv 1 \pmod 8$, k is a quadratic residue of 2^{α_1+1} for all non-negative integers α_1.

If $i > 1$ and $a^2 + k = (a - p_i^{\alpha_i})^2 + b^2$, then

$$b^2 = a^2 - (a - p_i^{\alpha_i}) + k = 2p_i^{\alpha_i}a - p_i^{2\alpha_i} + k$$

and hence k is a quadratic residue of $p_i^{\alpha_i}$. By Theorem 21, when λ_i is odd or k_i is a quadratic nonresidue of p_i, k is a quadratic residue of $p_i^{\alpha_i}$ if and only if $\alpha_i \leq \lambda_i$. When λ_i is even (including the case when $\lambda_i = 0$, i.e. when k is not divisible by p_i) and k_i is a quadratic residue of p_i, k is quadratic residue of $p_i^{\alpha_i}$ for all non-negative integers α_i.

So for each prime p_i, we can find an upper bound (may be infinity) for α_i's such that $p_i^{\alpha_i}$ is a possible value of l. By Theorem 31, $\prod p_i^{\alpha_i}$ is a possible value of l if all α_i's do not exceed the abovementioned upper bounds. For each possible values of l, k is a quadratic residue of l. So we can find square roots of k modulo l. Let θ be one of the square roots. If $b = lu + \theta$, then

$$\begin{aligned} a^2 + k &= (a - l)^2 + (lu + \theta)^2 \\ &= a^2 - 2al + l^2 + l^2u^2 + 2lu\theta + \theta^2 \\ 2al &= l^2\left(1 + u^2\right) + 2lu\theta + \theta^2 - k \\ a &= \frac{l(1 + u^2)}{2} + u\theta + \frac{\theta^2 - k}{2l} \end{aligned}$$

This give a solution to the equation if a is an integer. Note that $\dfrac{\theta^2 - k}{l}$ is an integer.

[18] Here we consider positive l only. As $a^2 = (-a)^2$ and $(a - l)^2 = (-a - (-l))^2$, solutions for negative l can be generate from solutions with positive l.

If both l and $\dfrac{\theta^2-k}{l}$ are even, then u can be any integer.

If both l and $\dfrac{\theta^2-k}{l}$ are odd, then u can be any even integer. Take $u=2t$.

$$a=\frac{l(1+4t^2)}{2}+2t\theta+\frac{\theta^2-k}{2l}=2lt^2+2t\theta+\frac{l}{2}+\frac{\theta^2-k}{2l}$$

If l is odd and $\dfrac{\theta^2-k}{l}$ is even, then u can be any odd integer. Take $u=2t+1$.

$$a=\frac{l(2+4t+4t^2)}{2}+(2t+1)\theta+\frac{theta^2-k}{2l}=2lt^2+2(l+\theta)t+l+\theta+\frac{\theta^2-k}{2l}$$

If l is even and $\dfrac{\theta^2-k}{l}$ is odd , then a is impossible to be an integer.

l	$\frac{\theta^2-k}{l}$	Corresponding solution (a,b)
odd	even	$\left(2lt^2+2(l+\theta)t+l+\theta+\frac{\theta^2-k}{2l}, 2lt+l+\theta\right)$
odd	odd	$\left(2lt^2+2t\theta+\frac{l}{2}+\frac{\theta^2-k}{2l}, 2lt+\theta\right)$
even	even	$\left(\frac{lt^2}{2}+t\theta+\frac{l}{2}+\frac{\theta^2-k}{2l}, lt+\theta\right)$
even	odd	no corresponding solution

TABLE 12. Solutions of $a^2+k=(a-l)^2+b^2$ corresponding to square root θ of k module l

Example 41. *Solve* $a^2-180=(a-l)^2+b^2$.

Take $k=-180=-1\cdot 2^2\cdot 3^2\cdot 5^1$.
Since $\lambda_1=2$ *is even and* $k_1=\dfrac{-180}{2^2}=-45\equiv 3\pmod 4$, $\alpha_1\le\lambda_1=2$.
Since $\lambda_2=2$ *is even and* $k_2=\dfrac{-180}{9}=-20$, $\left(\dfrac{k_2}{p_2}\right)=\left(\dfrac{-20}{3}\right)=\left(\dfrac{1}{3}\right)=1$. α_2 *can be any positive integer.*
Since $\lambda_3=1$ *is odd,* $\alpha_3\le\lambda_3=1$.
Note that

$$\left(\frac{k}{p_i}\right)=\left(\frac{2}{p_i}\right)^2\left(\frac{3}{p_i}\right)^2\left(\frac{-5}{p_i}\right)=\left(\frac{-5}{p_i}\right)$$

With reference to TABLE 11, $\left(\dfrac{k}{p_i}\right)=1$ *if and only if* $p_i\equiv 1,3,7,9\pmod{20}$.
So for $i\ne 1,2,3$, α_i *can be any non-negative integer if and only if* $p_i\equiv 1,3,7,9 \pmod{20}$.
Possible l *are those of the form* $\prod p_i^{\alpha_i}$, *where* α_i *are non-negative integers such that* $\alpha_1\le 2$, $\alpha_3\le 1$, *and* $\alpha_i=0$ *if* $i\ne 1,3$ *and* p_i *is not congruent to* 1, 3, 7, 9 *modulo* 20.
All possible values of l *under* 100 *are* 1, 2, 3, 4, 5, 6, 7, 9, 10, 12, 14, 15, 18, 20, 21, 23, 27, 28, 29, 30, 35, 36, 41, 42, 43, 45, 46, 47, 49, 54, 58, 60, 61, 63, 67, 69, 70, 81, 82, 83, 84, 86, 87, 89, 90, 92, 94, 98.
For example, take $l=21$. *If* $\theta^2\equiv -180\equiv 9\pmod{21}$, $\theta\equiv\pm 3\pmod{21}$. *The corresponding solution is* $(a,b,l)=(42t^2\pm 6t+15, 42t\pm 3, 21)$.
Take $l=23$. *If* $\theta^2\equiv -180\equiv 4\pmod{23}$, *then* $\theta\equiv\pm 21\pmod{23}$. *The corresponding solution is* $(a,b,l)=(46t^2\pm 42t+25, 46t\pm 21, 23)$.
Take $l=28$. *If* $\theta^2\equiv -180\equiv 16\pmod{28}$, *then* $\theta\equiv\pm 4,\pm 10\pmod{23}$. *The corresponding solution is* $(a,b,l)=(14t^2\pm 10t+19, 28t\pm 10, 28)$.

As $l = 28$ *is even and* $\dfrac{\theta^2 - k}{l} = \dfrac{(\pm 4)^2 - (-180)}{28} = 7$ *is odd,* $\theta = \pm 4$ *do not correspond to any solution.*

7. Conclusion

When h is a perfect square and k is an arbitrary integer, we can find all h, k-triples of form $(a^2, a^2 + h, a^2 + k)$ by solving $a^2 + k = (a - l)^2 + b^2$. For any solution of the equation, k is a quadratic residue of l. Given a particular k, we can use the method in Chapter 6 to find all possible factors of l.

If p is a prime number and p^λ is (but $p^{\lambda+1}$ is not) a factor of k, then p can be a factor of l, and the highest power of p as a factor of k is determined by two components, the parity of λ and the value of $\dfrac{k}{p^\lambda}$. If λ is odd, then the highest power is λ (or $\lambda - 1$ if $p = 2$). If $p = 2$ and λ is even, the highest power is decided by the remainder when $\dfrac{k}{p^\lambda}$ is divided by 8. When the remainder is 1, any power of 2 is a possible factor of l. If p is an odd prime and λ is even, the highest power of p as a factor of l is λ if and only if k is a quadratic nonresidue of p. When k is a quadratic residue of p, any power of p is a possible factor of l. If q is a prime number that is not a factor of k, then q (and any power of q) is a possible factor of l if and only if q is a quadratic residue of p.

We can use the abovementioned method to find all possible values of l. For a particular l, k is a quadratic residue of l and we can find square roots of k modulo l.[See reviewer's comment (19)] All possible values of a and b corresponding to this l can be found in terms of the square roots.

The following tables show all possible prime factors (and its maximum possible power) of l for some values of k.

k	possible prime factors of l (maximum possible power in bracket)	prime q (and all its powers) that can be a factor of l
1		all primes
2		$q \equiv \pm 1 \pmod 8$
3	3(1)	$q \equiv \pm 1 \pmod{12}$
4		all primes
5	2(1), 5(1)	$q \equiv \pm 1 \pmod 5$
6	3(1)	$q \equiv \pm 1, \pm 5 \pmod{24}$
7	7(1)	$q \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$
8	2(2)	$q \equiv \pm 1 \pmod 8$
9		all primes
10	5(1)	$q \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$
11	11(1)	$q \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \pmod{44}$
12	2(2), 3(1)	$q \equiv \pm 1 \pmod{12}$
13	2(1), 13(1)	$q \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$
14	7(1)	$q \equiv \pm 1, \pm 5, \pm 9, \pm 11, \pm 13, \pm 25 \pmod{56}$
15	3(1), 5(1)	$q \equiv \pm 1, \pm 7, \pm 11, \pm 17 \pmod{60}$
16		all primes
17	17(1)	$q \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17}$
18	3(2)	$q \equiv \pm 1 \pmod 8$
19	19(1)	$q \equiv \pm 1, \pm 3, \pm 5, \pm 9, \pm 15, \pm 17, \pm 25, \pm 27, \pm 31 \pmod{76}$
20	2(3), 5(1)	$q \equiv \pm 1 \pmod 5$

TABLE 13. Possible factors of l for positive k

k	possible prime factors of l (maximum possible power in bracket)	prime q (and all its powers) that can be a factor of l
-1		$q \equiv 1 \pmod 4$
-2		$q \equiv 1, 3 \pmod 8$
-3	2(1), 3(1)	$q \equiv 1 \pmod 3$
-4	2(2)	$q \equiv 1 \pmod 4$
-5	5(1)	$q \equiv 1, 3, 7, 9 \pmod{20}$
-6	3(1)	$q \equiv 1, 5, 7, 11 \pmod{24}$
-7	7(1)	$q \equiv 1, 2, 4 \pmod 7$
-8	2(2)	$q \equiv 1, 3 \pmod 8$
-9	3(2)	$q \equiv 1 \pmod 4$
-10	5(1)	$q \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}$
-11	2(1), 11(1)	$q \equiv 1, 3, 4, 5, 9 \pmod{11}$
-12	2(3), 3(1)	$q \equiv 1 \pmod 3$
-13	13(1)	$q \equiv 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49 \pmod{52}$
-14	7(1)	$q \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}$
-15	3(1), 5(1)	$q \equiv 1, 2, 4, 8 \pmod{15}$
-16	2(4)	$q \equiv 1 \pmod 4$
-17	17(1)	$q \equiv 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63 \pmod{68}$
-18		$q \equiv 1, 3 \pmod 8$
-19	2(1), 19(1)	$q \equiv 1, 5, 7, 9, 11, 17, 19, 23, 25, 35, 39, 43, 45, 47, 49, 55, 61, 63, 73 \pmod{76}$
-20	2(2), 5(1)	$q \equiv 1, 3, 7, 9 \pmod{20}$

TABLE 14. Possible factors of l for negative k

Appendix

The following table shows the distribution of $1,2$-triples and consecutive $1,2$-triples. $f(n)$ is the number of non-negative integers m not exceeding n such that m is the first number of an $1,2$-triple. $g(n)$ is the number of non-negative integers m not exceeding n such that both m and $m+8$ are the first numbers of $1,2$-triples. $h(n)$ is the number of non-negative integers m not exceeding n such that m, $m+8$ and $m+16$ are the first numbers of three $1,2$-triples.

n	$f(n)$	$g(n)$	$h(n)$
10	2	2	1
100	5	3	1
1000	14	5	1
10000	66	11	1
100000	446	30	1
1000000	3083	138	3
10000000	23140	767	7
100000000	183099	4635	21
1000000000	1490691	30865	144
2147483647	3008296	58450	244

TABLE 15

REFERENCES

[1] M. Aigner, and G.M. Ziegler, *Proofs from The Book*, Springer-Verlag, Berlin, 2004, 17-22. MR2014872

[2] E. J. Barbeau, *Pell's Equation*, Springer-Verlag, New York, 2003. MR1949691

[3] T. Cochrane, and R.E. Dressler,*Consecutive triples of sums of two squares*, Arch. Math. (Basel) **49** (1987), no. 4, 301-304, DOI 10.1007/BF01210713. MR913160

[4] C. Hooley, *On the intervals between numbers that are sums of two squares. II*, J. Number Theory, **5** (1973), no. 3, 215-217, DOI 10.1016/0022-314X(73)90046-2. MR0325557

[5] K. Kedlaya, *The 61st William Lowell Putnam Mathematical Competition*, http://kskedlaya.org/putnam-archive/2000.pdf

[6] K. S. Kedlaya, B. Poonen, and R. Vakil,*The William Lowell Putnam mathematical competition 1985-2000: problems, solutions and commentary*, Mathematical Association of America, Washington, DC, 2002, 292-294. MR1933844

[7] K. S. Kedlaya, *The William Lowell Putnam Mathematical Competition*, http://kskedlaya.org/putnam-archive/putnam2000stats.html

[8] Mathoverflow *Tuples of sums of two squares*, http://mathoverflow.net/questions/38211/tuples-of-sums-of-two-squares

[9] ProofWiki, *Euler's Criterion*,
https://proofwiki.org/wiki/Euler%27s_Criterion
[10] ProofWiki, *Gauss's Lemma (Number Theory)*,
https://proofwiki.org/wiki/Gauss%27s_Lemma_(Number_Theory)
[11] ProofWiki, *Second Supplement to Law of Quadratic Reciprocity*,
https://proofwiki.org/wiki/Second_Supplement_to_Law_of_Quadratic_Reciprocity
[12] Wikipedia, *BrahmaguptaFibonacci identity*,
https://en.wikipedia.org/w/index.php?title=Brahmagupta%E2%80%93Fibonacci_identity
&oldid=725035711
[13] Wikipedia, *Chinese remainder theorem*,
https://en.wikipedia.org/w/index.php?title=Chinese_remainder_theorem&oldid=733540003
[14] Wikipedia, *Fermat's little theorem*,
https://en.wikipedia.org/w/index.php?title=Fermat%27s_little_theorem&oldid=734199786
[15] Wikipedia, *Wilson's theorem*
https://en.wikipedia.org/w/index.php?title=Wilson%27s_theorem&oldid=728717619
[16] Wikipedia, *Quadratic residue*,
https://en.wikipedia.org/w/index.php?title=Quadratic_residue&oldid=731287061
[17] Wikipedia, *Legendre symbol*,
https://en.wikipedia.org/w/index.php?title=Legendre_symbol&oldid=716380308
[18] Wikipedia, *Quadratic reciprocity*,
https://en.wikipedia.org/w/index.php?title=Quadratic_reciprocity&oldid=730845406
[19] Wikipedia, *Sum of two squares theorem*,
https://en.wikipedia.org/w/index.php?title=Special:CiteThisPage&page
=Sum_of_two_squares_theorem&id=729694794

Reviewer's Comments

General Comments

The flow of this report was generally well. The report first explained the history, and then presented the findings. The organization of the report was not very good. One needs some clarifications at certain parts.

The writing was good. Most of the sentences were grammatically correct.

In the abstract, the second result should be stated in a clearer way.

The beginning was introduction. The linkage between sections was missed. One expects that the aim of each chapter is stated in the introduction and also at the beginning of each chapter. Especially Chapter 4 contained a lot of technical details. The readers may get lost until they read Chapter 4.3. Some important equations should not be stated along without any elaboration. For instance, on page 164, $a^2 + k = (a - l)^2 + b^2$ this important equation appeared without any explanation. There is a strange comment on page 164 (lines 3): 'Many solutions... solutions.' The authors may want to say that the results haven't existed in the literature.

One would be better if the authors add some elaboration on each theorem rather than just state the theorem. General audience is not familiar with the definition of square root of 2 modulo l where l is a positive integer. The authors may include the definition in the report.

The explanations in proofs were adequate and detailed. Some isolated equations in the proofs without explaining the logical relationship between them were found. One should pay more attention on Theorem 21 as in its proof the organization was unsatisfactory. Theorem 21 consisted of six statements, but the proof was not divided into six self-contained parts. The strategies of six proofs were similar, so one suggests that the authors explain the idea first, and then keep on applying to each statement. In this report a lot of equations were used repeatedly. One suggests that a label should be given to some commonly used equations.

In Section 5.1, what are the purposes of Examples 34 & 35? In Chapter 6.1, what are the purpose of those examples? How do we get Tables 10, 11, 13 & 14? In Section 6.3, symbol $\prod$ appeared several times. $\prod$ can be viewed as an infinite product but in the report we believe that the product is restricted as a finite product. Please pay some attention on Example 41.

In Example 41, it is demonstrated to solve a diophantine equation. However in its solution, it seems that a completed solution was not found. In Tables 13 & 14, the discussion about prime 2 did not appear. What is the reason?

In Chapter 6, the authors aimed to show Littlewood's problem in general. The report gave a theoretical solution but this solution heavily depends on the choices of l. It seems that the practical use of solution was not enough.

The citation was generally well. It would be better if the citing source is included in the sentence. One finds that a lot of citing sources in the report were put beyond the fullstops. A similar problem was also find when using the foot-note. Please check these throughout the report.

1,2-triple used the article 'an' instead of 'a'. Is it true?

For a report of such large number of pages, some typographical and minor mistakes are unavoidable. In the next section some spotted mistakes/ comments will be marked.

Mistakes

1. change 'has solutions' to 'is solvable' (?)
2. change 'as otherwise' to 'otherwise' (?)
3. change 'only possible' to 'all possible' (?)
4. 'There are ... 1,2-triples.' trivial or known (?)
5. change 'It is proved in Chapter 3 that' to 'Theorem 6 tells us that' (?)
6. '$r - s$ must be divisible by p' how can this achieve?
7. when $p = 3$, $\{2, 3, 4, \ldots, p-2\}$ =?
8. what if $p = 3$?
9. What does $\left\lfloor \frac{uq}{p} \right\rfloor$ mean?
10. insert 'Now we proceed to the discussion of prime powers.' (?)
11. change 'n^2' to 'then n^2' (?)
12. change '$\frac{(\theta-l)^2-2}{l}$' to 'then $\frac{(\theta-l)^2-2}{l}$' (?)
13. we should handle it by cases: Case I: $\left(\frac{3}{p}\right) = 1$ & Case II: $\left(\frac{3}{p}\right) = -1$
14. by LCM? by Chinese Remainder Theorem?
15. by hand?
16. insert 'Let us prove this result.' (?)
17. insert 'Let us explain this through Examples 39 & 40.'(?)
18. change 'first ... l' to 'considering the prime powers factor of l' (?)
19. change 'find square' to 'find all the square' (?)