When do we have $1 + 1 = 11$ and $2 + 2 = 5$?

“Freedom is slavery. Two and two make five.” - 1984.

R. PADMANABHAN
ALOK SHUKLA

The phrase “$2 + 2 = 5$” is a cliché or a slogan used in political speeches, propaganda, or literature, most notably in the novel “1984” by George Orwell. More recently, we came across a YouTube short film comedy, Alternative Math, produced by IdeaMan Studios (see [1]). It is a hilarious exaggeration of a teacher who is dragged through the mud for teaching that $2 + 2 = 4$ and not $22$, as Danny, a young student, kept on insisting. In the movie, Danny and the whole community sincerely believe $1 + 1 = 11$ and $2 + 2 = 22$. Jokes aside, we ask the question whether a polynomially defined group law “⊕” defined over the field of rationals such that $1 ⊕ 1 = u$ and $2 ⊕ 2 = v$ can simultaneously be satisfied for arbitrary integers $u$ and $v$. Answer to this question takes us through a fascinating journey from Brahmagupta all the way to the modern works of Louis Joel Mordell and Ramanujan!

1 Introduction.

In the standard mathematical world of arithmetic, the truth of ‘two plus two equals four’ is self-evident. However, a protagonist in the ‘Notes from the Underground’, by Fyodor Dostoevsky says:

“I admit that twice two makes four is an excellent thing, but if we are to give everything its due, twice two makes five is sometimes a very charming thing too.”

Taking inspiration from the works of fiction by Orwell and Dostoevsky, we ask rather seriously: can we really have $2 + 2 = 5$? If yes, then what about $1 + 1$ in such a mathematical system? And, what if we desire both $1 + 1 = 11$ and $2 + 2 = 5$ to hold together? ¹

¹In 2017, while election campaigning in the state of Gujarat, India, the Indian Prime Minister Narendra Modi declared, “1+1 is not 2 but 11 and together we will take Gujarat to new
Here we ask a more general question: when does the group law “⊕” satisfy both $1 \oplus 1 = u$ and $2 \oplus 2 = v$? To investigate this, let us fix a field $K$. The case of interest for us will be when $K$ is a finite extension of $\mathbb{Q}$. We will mainly consider the case of trivial extension, i.e., when $K = \mathbb{Q}$. We further impose the condition that $\oplus$ is defined by a polynomial $P(x, y) \in K[x, y]$, i.e., $x \oplus y = P(x, y)$. Our main goal will be to answer the following two questions.

(1) Given $u$ and $v$, find $P$ and $K$ such that $1 \oplus 1 = u$ and $2 \oplus 2 = v$?

(2) Given some conditions on $u$ and $v$, and $K = \mathbb{Q}$, will it be possible to have $1 \oplus 1 = u$ and $2 \oplus 2 = v$?

**Definition 1** Let $K$ be a finite extension of $\mathbb{Q}$. We say that $(u, v, P, K)$ is true, if there exists a commutative group operation $x \oplus y$ given by a polynomial $P(x, y) \in K[x, y]$, such that

$$1 \oplus 1 = u \quad \text{and} \quad 2 \oplus 2 = v.$$  \hfill (1)

2 Characterization of the polynomial group operation $x \oplus y = P(x, y)$.

In order to address the questions raised in the previous section, we will first characterize the polynomial $P(x, y)$, using the commutative and associative properties of the group law $\oplus$. Suppose the highest degree of $x$ in $P(x, y)$ is $n$. Then, associativity of $P(x, y)$ implies $P(P(x, y), z) = P(x, P(y, z))$. The highest degree of $x$ on the left is $n^2$, whereas it is $n$ on the right side. Therefore, $n^2 = n$. We ignore the case $n = 0$, as it will mean that $P(x, y)$ doesn’t depend on $x$. A contradiction, since the group operation $\oplus$ must depend on both $x$ and $y$. Similarly, the highest degree of $y$ in $P(x, y)$ is also 1. Next, commutativity of $P(x, y)$ implies that $P(x, y)$ is symmetric in $x$ and $y$, hence it can be assumed that

$$P(x, y) = axy + bx + by + c.$$  \hfill (2)
When do we have $1 + 1 = 11$ and $2 + 2 = 5$?

Using associativity, we write $(1 \oplus 2) \oplus 3 = 1 \oplus (2 \oplus 3)$. Now

$$P(P(1, 2), 3) = P(1, P(2, 3))$$

$$\implies (2a + 3b + c, 3) = P(1, 6a + 5b + c)$$

$$\implies 3a(2a + 3b + c) + b(2a + 3b + c + 3) + c$$

$$= a(6a + 5b + c) + b(6a + 5b + c + 1) + c$$

$$\implies ac = b^2 - b. \quad (3)$$

If $a = 0$, then $b$ must be 1 as both $a$ and $b$ can’t be zero simultaneously. Therefore, there are two possibilities for $P(x, y)$. Either,

$$P(x, y) = x + y + c, \quad (4)$$

or else, if $a \neq 0$ then

$$P(x, y) = axy + bx + by + \frac{b^2 - b}{a}. \quad (5)$$

**Remark** See the proof of Lemma 5, [3], for a similar proof of the above result.

The former case, $P(x, y) = x + y + c$ is easy to deal with, and we immediately dispose it of. It is clear that in this case $1 \oplus 1 = u$ and $2 \oplus 2 = v$ implies that $2 + c = u$ and $4 + c = v$. But then $v - u = 2$. Therefore, we conclude that:

**Lemma 1** If $u, v \in \mathbb{Q}$ be such that $v - u = 2$, then there exists a group operation $\oplus$, given by the polynomial $x \oplus y = P(x, y) = x + y + u - 2$, such that $1 \oplus 1 = u$ and $2 \oplus 2 = v$, i.e., $(u, u + 2, x + y + u - 2, \mathbb{Q})$ is true.

**Remark** We note here that $x \oplus y = P(x, y)$ given by Eq. (4) and Eq. (5), both define a group. It can directly be checked that $-c$ is the identity element in the former case and $\frac{1-b}{a}$ is the identity elements in the later case. Moreover, it is interesting to note that the group obtained is isomorphic to $K$ in the former case, whereas the group obtained in the later case is isomorphic to the multiplicative group of the non-zero elements of the field, i.e., $K^\times$. The isomorphism in the case when $P(x, y)$ is defined by Eq. (5), is given by $f(x) = ax + b$ as shown below.

$$f(P(x, y)) = aP(x, y) + b$$

$$= a(axy + bx + by + (b^2 - b)/a) + b$$

$$= a^2 xy + abx + aby + (b^2 - b) + b$$

$$= (ax + b)(ay + b)$$

$$= f(x) \times f(y).$$
This proves the isomorphism. In particular, to find the identity element e, we simply solve the equation \( f(e) = 1 : ae + b = 1 \), or \( e = (1 - b)/a \). Moreover, the inverse of 0 \( \in K \) under the map \( f \) is \(-b/a\), therefore, the group given by \( x \oplus y = P(x, y) = axy + bx + by + (b^2 - b)/a \) is defined on the set \( K - \{ -b/a \} \).

In the following, we will continue to use the statement ‘\((u, v, P, K)\) is true’ as defined in Def. 1, even when the group might be defined on the set \( K - \{ -b/a \} \), rather than on \( K \).

### 3 Connections with number theory.

Now we consider the other more interesting case \( a \neq 0 \), and assume that \( P(x, y) \) is given by Eq. (5). Since, from Eq. (1), we have \( 1 \oplus 1 = u \), and \( 2 \oplus 2 = v \), we need to solve for \( a, b \), in the following equations:

\[
\begin{align*}
    a^2 - b + 2ab + b^2 &= au, \\
    4a^2 - b + 4ab + b^2 &= av.
\end{align*}
\]

Subtracting Eq. (6) from Eq. (7) gives,

\[
3a^2 + 2ab = a(v - u)
\]  

Since \( a \neq 0 \) by assumption, Eq. (8) implies \( 3a + 2b = v - u \), or \( b = \frac{1}{2}(-3a - u + v) \).

Substituting \( b = \frac{1}{2}(-3a - u + v) \) in Eq. (6) leads to a quadratic equation in \( a \), which can easily be solved. We note the final solutions \(^2\)

\[
\begin{align*}
    a &= -3 + u + v \pm \sqrt{9 - 8u - 4v + 4uv} \quad \text{and} \quad b = \frac{1}{2}(-3a - u + v).
\end{align*}
\]

For \( u = 11 \) and \( v = 5 \), from the above equation, we see that the solution is possible in \( \mathbb{Q} \), i.e., \((11, 5, 24xy - 39x - 39y + 65, \mathbb{Q})\) is true. As remarked earlier, we note that \(-b/a = 39/24\) is excluded from \( \mathbb{Q} \), while defining the group in this example. However, it is not always possible to have \( 1 \oplus 1 = u \) and \( 2 \oplus 2 = v \), defined by a polynomial group law \( \oplus \) over rationals, i.e., \((u, v, P, \mathbb{Q})\) is not always true. As an example, for \( u = 11 \) and \( v = 22 \) we have

\[
a = 3(10 \pm \sqrt{89}) \quad \text{and} \quad b = \frac{1}{2}(11 - 3a).
\]

\(^2\)One can use the Mathematica code \texttt{solve(resultant(a^2 - b + 2ab + b^2 - au, 4a^2 - b + 4ab + b^2 - av, b), a)} to get \( a \) as given in Eq. (9).
When do we have $1 + 1 = 11$ and $2 + 2 = 5$?

In this case, $(11, 22, P, Q)$ is false, but $(11, 22, P, Q(\sqrt{89}))$ is true, answering Danny’s question, [1].

Now we consider, given $u, v \in \mathbb{Z}$, whether $(u, v, P, Q)$ is true (with $P$ as defined in Eq. (5)). It is clear that for $(u, v, P, Q)$ to be true $9 - 8u - 4v + 4uv$ must be perfect square. Consider the Diophantine equation

$$9 - 8u - 4v + 4uv = n^2.$$  \(10\)

for all possible integers $u, v$ and $n$. First we assume that $n$ is fixed. Clearly for a solution to exist $n^2 \equiv 1 \mod 4$. This means $n$ must be odd. Then, in fact, $n^2 \equiv 1 \mod 8$. Let this be the case. Assume $n = 2m + 1$. Then, we have

$$2 - 2u - v + uv = m(m + 1) \implies (u - 1)(v - 2) = m(m + 1) = \frac{1}{4}(n^2 - 1).$$  \(11\)

From Eq. 11, for a given $n$ we can count the number of solutions $(u, v)$, and it is given by $\sigma_0(\frac{1}{4}(n^2 - 1)) = $ the number of divisors of $\frac{1}{4}(n^2 - 1)$.

Next, we assume that $u, v$ are given. From Eq. (11), a necessary condition for $(u, v, P, Q)$ to be true is

$$(u - 1)(v - 2) \equiv 0 \mod 2.$$  \(12\)

Since, $n$ is odd, $\frac{n^2 - 1}{4} \geq 0$. This means $(u - 1)(v - 2) \geq 0$.

Now we will prove a number of results characterizing the truth of $(u, v, P, Q)$.

**Theorem 1**

(i) Let $u - 1$ and $v - 2$ be prime numbers. Then,

$$(u, v, P, Q) \text{ is true (clarify Def. 1)} \implies u = v = 4 \text{ or } u = 3, v = 5.$$  \(13\)

(ii) $|u - v + 1| = 1 \implies (u, v, P, Q) \text{ is true }.$

**Proof**

(i) Since, $(u, v, P, Q)$ is true, from Eq. (11),

$$(u - 1)(v - 2) = \left(\frac{n - 1}{2}\right)\left(\frac{n + 1}{2}\right).$$  \(14\)
Since, \( \gcd\left(\frac{u+1}{2}, \frac{v-1}{2}\right) = 1 \), we have the following cases:

\[
\begin{cases}
    u - 1 = \frac{u+1}{2} & \text{and } v - 2 = \frac{v-1}{2}, \\
    u - 1 = \frac{v-1}{2} & \text{and } v - 2 = \frac{u+1}{2}.
\end{cases}
\]

From the above, we get that \( \frac{u+1}{2} \) and \( \frac{v-1}{2} \) must be consecutive primes. This means \( \frac{u+1}{2} = 2 \) and \( n = 5 \). Then, either \( u = v = 4 \) or \( u = 3 \) and \( v = 5 \) and the proof is complete.

(ii) As \( |u - v + 1| = 1 \), we get either \( u = v \) or \( u = v - 2 \). If \( u = v \), then \( 9 - 8u - 4v + 4uv = (2u - 3)^2 \). Next, if \( u = v - 2 \), then \( 9 - 8u - 4v + 4uv = (2v - 5)^2 \). Therefore, in both the cases \( (u, v, P, \mathbb{Q}) \) is true, and we are done.

\( \square \)

Our next result is related to Pell’s equation, i.e., equation of the form \( n^2 - dt^2 = 1 \), where \( d \) is a fixed positive non-square integer, and integer solutions for \( (n, t) \) are sought. In order to solve Pell’s equation, it is helpful to consider the factorization \( n^2 - dt^2 = (n + \sqrt{d}t)(n - \sqrt{d}t) \). For simplicity assume \( d \) is square-free and also \( d \not\equiv 1 \mod 4 \). Then numbers of form \( n + \sqrt{d}t \) form a ring \( \mathbb{Z}[\sqrt{d}] \), which is the ring of integers for the number field \( \mathbb{Q}(\sqrt{d}) \). For an element \( z = n + \sqrt{d}t \), we define its conjugate as \( \bar{z} = n - \sqrt{d}t \). Then norm is defined as \( N(z) = z\bar{z} \). It is easy to see that norm is multiplicative, i.e., \( N(ab) = N(a)N(b) \) for \( a, b \in \mathbb{Z}[\sqrt{d}] \). Any \( z = n + \sqrt{d}t \) is a solution to Pell’s equation \( n^2 - dt^2 = 1 \), if \( N(z) = 1 \). Let \( \epsilon > 1 \) be the smallest number in \( \mathbb{Z}[\sqrt{d}] \), such that \( N(\epsilon) = 1 \), then \( \epsilon \) is a fundamental unit. Indeed, every unit of norm 1 is of the form of \( \pm \epsilon^k \) for some integer \( k \). To see this suppose that \( N(z) = 1 \).

If necessary replacing \( z \) by \( -z \), we can assume \( z > 0 \). There exist a unique integer \( k \) such that \( \epsilon^k \leq z < \epsilon^{k+1} \). Then \( N(\epsilon^{-k}z) = N(\epsilon)^{-k}N(z) = 1 \) and \( 1 \leq \epsilon^{-k}z < \epsilon \). Thus the existence of \( \epsilon_1 = \epsilon^{-k}z \) contradicts the minimality of \( \epsilon \) unless \( \epsilon_1 = 1 \). Assuming this to be the case, we obtain \( z = \epsilon^k \), as claimed.

Now we give our next result.

**Theorem 2** If \( (u - 1)(v - 2) = 2t^2 \), where \( u, v \) and \( t > 0 \) are integers, then

\[
(u, v, P, \mathbb{Q}) \text{ is true (clarify Def. 1)} \iff t = \frac{(3 + 2\sqrt{2})^m - (3 - 2\sqrt{2})^m}{4\sqrt{2}} \quad (15)
\]

for some positive integer \( m \).
Proof Assume \((u, v, P, Q)\) to be true. Then from Eq. (11) and the given hypothesis 
\((u - 1)(v - 2) = 2t^2\), we obtain
\[
  n^2 - 8t^2 = 1.
\]
This is a special case of Pell’s equation \(n^2 - dt^2 = 1\), with \(d = 8\). In the number field 
\(K = \mathbb{Q}(\sqrt{2})\), we can write
\[
  (n + 2\sqrt{2}t)(n - 2\sqrt{2}t) = 1.\]
Then \(N(n + 2\sqrt{2}t) = 1\), where \(N(\cdot)\) is the usual norm in 
\(K\). We note that \(n = 3\), \(2t = 2\) is a solution of Eq. \(21\), and in fact, \(3 + 2\sqrt{2}\) is a fundamental unit (see Table 4, Page 280, [2]). Then from Theorem 11.3.2, [2], it follows that any solution of \(n^2 - 8t^2 = 1\), 
will be such that \(n + 2\sqrt{2}t = \pm(3 + \sqrt{2} \cdot 2)^m\) for some integer \(m\). We can assume 
\(m\) to be a positive integer. Then on solving for \(t\), in \(n + 2\sqrt{2}t = (3 + \sqrt{2} \cdot 2)^m\) and 
\(n - 2\sqrt{2}t = (3 + \sqrt{2} \cdot 2)^{-m} = (3 - \sqrt{2} \cdot 2)^m\), the result follows.

Now, to prove the other direction assume that \(t\) is given by Eq. (15). Then on defining 
\[
  n = \frac{(3 + 2\sqrt{2})^m + (3 - 2\sqrt{2})^m}{2},
\]
we see that \(n^2 - 8t^2 = 1\). This along with \((u - 1)(v - 2) = 2t^2\) gives 
\(u - 1)(v - 2) = \frac{t^2 - 1}{4}\). Then, \(9 - 8u - 4v + 4uv = n^2\). Therefore, \((u, v, P, Q)\) is true. This completes 
the proof for the other direction. 

Remark (Chakravala: an ancient algorithm.) We note that the proof of the above 
theorem depended upon the solution of Pell’s equation \(n^2 - 8t^2 = 1\). Indeed, Pell’s 
equation has a very interesting history. It is one of the cases of wrong attributions in mathematics.
In 1657 Fermat posed a challenge to mathematicians. The challenge was to find integer solutions for the equation \( x^2 - Ny^2 = 1 \), for values of \( N \) like \( N = 61, 109 \). Several centuries earlier, in 1150, Bhaskara II had already found solutions for the problem proposed by Fermat.

\[
\begin{align*}
1766319049^2 - 61(226153980)^2 &= 1 \\
158070671986249^2 - 109(15140424455100)^2 &= 1.
\end{align*}
\]

In fact, Brahmagupta (598–665) had already solved this equation in the early seventh century for various values of \( N \), such as \( N = 83 \) and \( N = 92 \). Brahmagupta viewed these problems very highly and he had remarked: “Any person who is able to solve these two cases, within a year, is truly a mathematician”!

Let \((a, b; m)\) to denote an integer solution of the equation \( x^2 - Ny^2 = m \). Brahmagupta discovered the following ‘composition rule’ in the early seventh century.

\[
(a, b; m) \ast (c, d; n) \rightarrow (ac \pm Nbd, ad \pm bc; mn). \tag{19}
\]

This is perhaps one of the earliest example of the use a ‘group-theoretic’ argument in mathematics. This ‘composition rule’ allowed Brahmagupta to obtain new solutions from old known solutions, since clearly by composing a known solution \((a, b; m)\) with a triple \((p, q; 1)\), one can easily find new solutions \((ap \pm Nbq, aq \pm bp; n)\). Later, Jayadeva, Narayana and Bhaskara had refined and built on the works of Brahmagupta to devise an algorithm called the “Chakravala” for finding all the integer solutions of the equation \( x^2 - Ny^2 = \pm 1 \) for any positive integer \( N \). We refer readers to [6] for an interesting discussion on this.

**Theorem 4** If \((u - 1)(v - 2) = 2t^3\), where \( u, v \) and \( t \) are integers, then

\[
(u, v, P, \mathbb{Q}) \text{ is true (clarify Def. 1)} \iff t = 0 \text{ or } t = 1. \tag{20}
\]

**Proof** From \((u - 1)(v - 2) = \frac{1}{4}(n^2 - 1)\) we need to solve,

\[
n^2 = (2t)^3 + 1. \tag{21}
\]

This is a special case of Mordell’s equation \( y^2 = x^3 + k \), with \( k = 1 \). It is known that only integral solutions of this equation are \((x, y) = (-1, 0), (0, \pm 1)\), and \((2, \pm 3)\) (See Theorem 5, Chapter 26, Page 247, [4]).

For example, we see that if \( t = 0 \), then \((u - 1)(v - 2) = 0\). Suppose, \( u = 1 \). Then from Eq. (9) we get \((a, b) = (v - 1, 1 - v)\) or \((a, b) = (v - 3, 4 - v)\) and \( P(x, y) \) as
When do we have $1 + 1 = 11$ and $2 + 2 = 5$? 

given in Eq. (5) is a rational polynomial. Similarly, if $v = 2$ then from Eq. (9) we get $(a, b) = (u, 1 - 2u)$ or $(a, b) = (u - 2, 4 - 2u)$ and $P(x,y)$ is again a rational polynomial in this case.

**Theorem 5** If $(u - 1)(v - 2) = 2(2^{t-3} - 1)$, where $u, v$ and $t$ are integers with $t > 1$, then

$$(u, v, P, \mathbb{Q}) \text{ is true (clarify Def. 1)} \iff t \in \{3, 4, 5, 7, 15\}. \quad (22)$$

**Proof** First let $(u, v, P, \mathbb{Q})$ be true. Then from Eq. (11) and the given hypothesis $(u - 1)(v - 2) = 2(2^{t-3} - 1)$, we get

$$n^2 + 7 = 2^t. \quad (23)$$

We recall this is Ramanujan-Nagell equation. In fact, Ramanujan conjectured in 1913 that $(1, 3), (3, 4), (5, 5), (11, 7)$ and $(181, 15)$ are only positive solutions $(n, t)$ of the Diophantine equation $n^2 + 7 = 2^t$. Nagell proved this conjecture in 1948, [5]. Therefore, from this our result follows.

Finally, we would like to add yet another “strange” multiplication $\oplus$ corresponding to the case of $t = 4$ of the Ramanujan-Nagell equation. In this case $u = 2, v = 4$, and the group law is

$$x \oplus y = 6xy - 8x - 8y + 12.$$ 

Here we have $1 \oplus 1 = 2$ and $2 \oplus 2 = 4$, which looks like the ordinary addition, but it is a different group operation. The element $\frac{4}{3}$ is an “annihilator” of the group because:

$$x \oplus \frac{4}{3} = 8x - 8x - 8 \times \left(\frac{4}{3}\right) + 12 = \frac{4}{3}.$$ 

**References**

[1] Alternative math: Short film, https://youtu.be/Zh3Yz3PiXZw, uploaded on: Sept.19, 2017.
[2] Saban Alaca and Kenneth S Williams. *Introductory algebraic number theory*. Cambridge University Press, 2004.
[3] Joel V Brawley, Shuhong Gao, and Donald Mills. Associative rational functions in two variables. In *Finite Fields and Applications*, pages 43–56. Springer, 2001.
[4] Louis Joel Mordell. *Diophantine equations*, volume 30. Academic Press, 1969.
[5] T Nagell. The Diophantine equation $x^2 + 7 = 2^n$. *Arkiv för Matematik*, 4(2):185–187, 1961.
[6] André Weil. *Number Theory: An approach through history from Hammurapi to Legendre*. Springer Science & Business Media, 2006.
R. Padmanabhan and Alok Shukla

Department of Mathematics, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada
Mathematical and Physical Sciences division, Ahmedabad University, India
padman@cc.umanitoba.ca, Alok.Shukla@ahduni.edu.in