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

R. Padmanabhan
Alok Shukla

This work is inspired in part by the following passage from the famous dystopian novel 1984, by George Orwell:
"*He wrote first in large clumsy capitals: FREEDOM IS SLAVERY.*
Then almost without a pause he wrote beneath it: TWO AND TWO MAKE FIVE".

Here we address a more general question: when does the group law "+", defined using a polynomial, on the set of rational numbers, satisfy both 1+1=u and 2+2=v? Surprisingly, this innocuous and perhaps strange looking question, has connections with some interesting results in number theory, going back to the work of Indian mathematician Brahmagupta, from the early 7th century.

1 Introduction.

Imagine a world where two plus two may not equal four. Such a world was depicted in the novel 1984, by George Orwell, wherein under a powerful oppressing state the truth of "two and two make four" can no longer be taken for granted. We quote:

> *'You are a slow learner, Winston,' said O'Brien gently.*
> *'How can I help it?' he blubbered. 'How can I help seeing what is in front of my eyes? Two and two are four.'*
> *Sometimes, Winston. Sometimes they are five. Sometimes they are three. Sometimes they are all of them at once. You must try harder. It is not easy to become sane.'*

Of course, 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 above 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]

Here we ask a more general question: when does the group law "$\oplus$" 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 is $\mathbb{Q}$. 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 $(\mathbf{u}, \mathbf{v}, \mathbf{P}, \mathbf{K})$ **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

$$1 \oplus 1 = u \qquad \text{and} \qquad 2 \oplus 2 = v. \tag{1}$$

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

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,

[1] In 2017, while election campaigning in the state of Gujarat, India, the then Indian Prime Minister Narendra Modi declared, "1+1 is not 2 but 11 and together we will take Gujarat to new heights". Another political leader, the general secretary of Communist Party of India (Marxist), Mr. Sitaram Yechury said in 2017: "Politics is not just arithmetic. Two plus two could become twenty two if we strengthened people's struggle." See also a funny math video [1].

commutativity of $P(x,y)$ implies that $P(x,y)$ is symmetric in x and y, hence it can be assumed that

$$P(x,y) = axy + bx + by + c. \tag{2}$$

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

$$\begin{aligned}
&P(P(1,2),3) = P(1,P(2,3)) \\
&\implies (2a+3b+c,3) = P(1,6a+5b+c) \\
&\implies 3a(2a+3b+c) + b(2a+3b+c+3) + c \\
&\qquad\qquad = a(6a+5b+c) + b(6a+5b+c+1) + c \\
&\implies ac = b^2 - b. \qquad (3)
\end{aligned}$$

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,

$$P(x,y) = x + y + c, \tag{4}$$

or else, if $a \neq 0$ then

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

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 off. 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 $v - u = 2$. The converse is also obvious. 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.

$$\begin{aligned} f(P(x,y)) &= aP(x,y) + b \\ &= a(axy + bx + by + (b^2 - b)/a) + b \\ &= a^2xy + abx + aby + (b^2 - b) + b \\ &= (ax + b)(ay + b) \\ &= f(x) \times f(y). \end{aligned}$$

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:

$$a^2 - b + 2ab + b^2 = au, \tag{6}$$

$$4a^2 - b + 4ab + b^2 = av. \tag{7}$$

Since $a \neq 0$ by assumption, the only solutions obtained are

$$a = -3 + u + v \pm \sqrt{9 - 8u - 4v + 4uv} \qquad \text{and} \qquad b = \frac{1}{2}(-3a - u + v). \tag{8}$$

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

$$a = 3(10 \pm \sqrt{89}),\ b = \frac{1}{2}(11 - 3a).$$

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

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

$$9 - 8u - 4v + 4uv = n^2. \tag{9}$$

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

$$\begin{aligned} 2 - 2u - v + uv &= m(m+1) \\ \implies (u-1)(v-2) &= m(m+1) = \frac{1}{4}(n^2 - 1). \end{aligned} \tag{10}$$

From Eq. 10, 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. (10), a necessary condition for $(u, v, P, \mathbb{Q})$ to be true is

$$(u-1)(v-2) \equiv 0 \mod 2. \tag{11}$$

We also note that, if $(u-1)(v-2) < 0$, then from Eq. (10), we conclude $\frac{n^2-1}{4} < 0$, for $(u, v, P, \mathbb{Q})$ to be true. Then $n = 0$ or $n = \pm 2$, as n must be odd. Clearly, for these values of n, there does not exist any integer solution for u, v, satisfying Eq. (10). Therefore, $(u, v, P, \mathbb{Q})$ is false.

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

Theorem 1

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

$$(u, v, P, \mathbb{Q}) \text{ is true (clarify Def. 1)} \implies u = v = 4 \text{ or } u = 3, v = 5. \tag{12}$$

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

Proof

(i) Since, $(u, v, P, \mathbb{Q})$ is true, from Eq. (10),

$$(u-1)(v-2) = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right). \tag{13}$$

Since, $\gcd(\frac{n+1}{2}, \frac{n-1}{2}) = 1$, we have the following cases:

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

From the above, we get that $\frac{n-1}{2}$ and $\frac{n+1}{2}$ must be consecutive primes. This means $\frac{n-1}{2} = 2$ 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.

□

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

$$(u, v, P, \mathbb{Q}) \text{ is true (clarify Def. 1)} \iff t = \frac{(3+2\sqrt{2})^m - (3-2\sqrt{2})^m}{4\sqrt{2}} \tag{14}$$

for some positive integer m.

Proof Assume $(u, v, P, \mathbb{Q})$ to be true. Then from Eq. (10) and the given hypothesis $(u-1)(v-2) = 2t^2$, we obtain

$$n^2 - 8t^2 = 1. \tag{15}$$

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. 20, 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. (14). Then on defining

$$n = \frac{(3+2\sqrt{2})^m + (3-2\sqrt{2})^m}{2}, \tag{16}$$

we see that $n^2 - 8t^2 = 1$. This along with $(u-1)(v-2) = 2t^2$ gives $(u-1)(v-2) = \frac{n^2-1}{4}$. Then, $9 - 8u - 4v + 4uv = n^2$. Therefore, $(u, v, P, \mathbb{Q})$ is true. This completes the proof for the other direction. □

We state the following result, whose proof is similar to the previous theorem.

Theorem 3 *Let $\alpha_d + \beta_d\sqrt{2d}$ be the fundamental unit of the number field $K = \mathbb{Q}(\sqrt{2d})$, where d is a square free odd integer. Also assume $(u-1)(v-2) = 2dt^2$, with u, v and $t > 0$ being integers. Then*

$$(u, v, P, \mathbb{Q}) \text{ is true (clarify Def. 1)} \iff t = \frac{(\alpha_d + \beta_d\sqrt{2d})^m - (\alpha_d - \beta_d\sqrt{2d})^m}{4\sqrt{2d}}, \tag{17}$$

for some positive integer m.

Remark (Chakravala: an ancient algorithm) We note that the proof of the above theorem depended upon the solution of Pell's equation $n^2 - 8dt^2 = 1$. 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.

$$1766319049^2 - 61(226153980)^2 = 1$$
$$158070671986249^2 - 109(15140424455100)^2 = 1.$$

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.

$$(a, b; m) * (c, d; n) \to (ac \pm Nbd, ad \pm bc; mn). \tag{18}$$

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*

$$(u,v,P,\mathbb{Q}) \text{ is true (clarify Def. 1)} \iff t = 0 \text{ or } t = 1. \tag{19}$$

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

$$n^2 = (2t)^3 + 1. \tag{20}$$

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]). □

Theorem 5 *If $(u-1)(v-2) = 2(2^{t-3}-1)$, where u, v and t are integers with $t > 0$, then*

$$(u,v,P,\mathbb{Q}) \text{ is true (clarify Def. 1)} \iff t \in \{3,4,5,7,15\}. \tag{21}$$

Proof First let $(u,v,P,\mathbb{Q})$ be true. Then from Eq. (10) and the given hypothesis $(u-1)(v-2) = 2(2^{n-3}-1)$, we get

$$n^2 + 7 = 2^t. \tag{22}$$

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. □

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.

University of Manitoba, Canada

Ranganathan.Padmanabhan@umanitoba.ca, sajal.eee@gmail.com