1.1 – Introduction

My essay is inspired by a question on the 2012 UKMT Senior Mathematical Challenge "which of the following numbers do *not* have a square root in the form $x + y\sqrt{k}$, where x and y are positive integers?", and amalgamates elementary number theory and discrete mathematics – my favourite areas of mathematics!

I will be exploring the nature of numbers in the form $a + b\sqrt{k}$, where a, b are non-zero integers and k is a non-square positive integer, namely its irrationality; what happens when it undergoes basic arithmetic operations; its integer powers and the relationship between $a + b\sqrt{k}$ and $\left(a + b\sqrt{k}\right)^n$; lastly, its minimal polynomial.

I want to reiterate that I will not be dealing with complex or non-integer rational numbers, or else this essay would be beyond the level of high school mathematics.

2.1 – Irrationality of $\boldsymbol{a + b\sqrt{k}}$

Irrational numbers are numbers that cannot be expressed as fraction. Due to the presence of a square root, it is safe to assume that $a + b\sqrt{k}$ is irrational. Also, the sum of an integer, a rational number, and an irrational number is always irrational, because if not, then the irrational number would be the difference of 2 rational numbers, which is rational, and thus, a contradiction (James Madison University , 2000). By a similar argument, $b\sqrt{k}$ is irrational if $\sqrt{k}$ is irrational (a rational number divided by some other rational number gives another rational number, suggesting that $\sqrt{k}$ would be rational, which is absurd and hence, a contradiction) (MathBitsNotebook). However, assuming here that $\sqrt{k}$ is irrational is not rigorous. Hence, by proving the irrationality of $\sqrt{k}$, we can prove that $a + b\sqrt{k}$ is also irrational.

Assume $\sqrt{k}$ is rational. $\sqrt{k}$ can then be expressed as $\frac{x}{y}$, where the greatest common divisor of p and q (gcd(p,q)) is 1.

$$\sqrt{k} = \frac{x}{y}$$

$$k = \frac{x^2}{y^2}$$

$$x^2 = ky^2$$

This means that k divides x^2.

From Euclid's lemma, if a prime number p divides x^2, then p also divides x. Thus, from the fundamental theorem of arithmetic, as k can be expressed uniquely as the product of its distinct prime factors p_i raised to a certain integer power q_i,

$$k = p_1^{q_1} \times p_2^{q_2} \times \ldots \times p_m^{q_m} \times \ldots \times p_s^{q_s} \times \ldots \times p_n^{q_n}$$ (where all $q_i \geq 1$ and there exists a q_i [let us call this q_s] that is odd, since k is a non-square)

there exists some prime p_m that divides both x and x^2. Moreover, when x^2 is expressed as the product of its primes, p_m must be raised to an even power, since p_m also divides x. As x and y are co-prime, x^2 and y^2 are also co-prime (Illinois University), which mean they share no common factors. This means that all prime factors raised to their respective powers, $p_i^{q_i}$, must divide x^2 fully, indicating that all q_i must be even. However, q_s is odd, which is a contradiction.

Hence, by proof by contradiction, the statement that "$\sqrt{k}$ is rational" is absurd, so $\sqrt{k}$ must be irrational, which confirms that $a + b\sqrt{k}$ is irrational.

2.2 – Basic Arithmetic Operations on $a + b\sqrt{k}$

Addition & Subtraction

Addition and subtraction on numbers in the form $a + b\sqrt{k}$ are very straightforward, just like normal integers:

$$(a_1 + b_1\sqrt{k}) + \left(a_2 + b_2\sqrt{k}\right) + \ldots + \left(a_n + b_n\sqrt{k}\right) = (a_1 + a_2 + \ldots + a_n) + (b_1 + b_2 + \ldots + b_n)\sqrt{k}$$
$$(a_1 + b_1\sqrt{k}) - \left(a_2 + b_2\sqrt{k}\right) - \ldots - \left(a_n + b_n\sqrt{k}\right) = (a_1 - a_2 - \ldots - a_n) + (b_1 - b_2 - \ldots - b_n)\sqrt{k}$$

We can see that when adding or subtracting two numbers in this form, a number in the same form is obtained. Hence, the set of numbers in the form $a + b\sqrt{k}$ is closed under addition (provided that $(a_1 + a_2 + \ldots + a_n), (b_1 + b_2 + \ldots + b_n) \neq 0$) and subtraction (provided that $(a_1 - a_2 - \ldots - a_n), (b_1 - b_2 - \ldots - b_n) \neq 0$). Furthermore, this also shows that if one wants to find two or more numbers in the form $a + b\sqrt{k}$ that add or subtract to give a number in same form with a and b given, they can compare coefficients to form an under-specified system of linear equations (only 1 linear equation in this case), which has infinite solutions.

Multiplication

Similarly, when multiplying two numbers in this form, a number in the same form is obtained:

$$\left(a_1 + b_1\sqrt{k}\right) \times \left(a_2 + b_2\sqrt{k}\right) = (a_1a_2 + b_1b_2k) + (a_1b_2 + a_2b_1)\sqrt{k}$$

As this number is also in the form $a + b\sqrt{k}$, since $a_1, b_1, a_2, b_2, \epsilon\ \mathbb{Z}$, $a = (a_1a_2 + b_1b_2)\ \epsilon\ \mathbb{Z}$ and $b = (a_1b_2 + a_2b_1)\ \epsilon\ \mathbb{Z}$. Thus, one can deduce that no matter how many times a number in this form is multiplied by another number in the same form, a number of the same form is always obtained, i.e. the set of numbers in the form $a + b\sqrt{k}$ is closed under multiplication as well.

Division

On the other hand, the nature of these numbers is a little more complicated with division:

$$\frac{(a_1+b_1\sqrt{k})}{(a_2+b_2\sqrt{k})} = \frac{(a_1+b_1\sqrt{k})(a_2-b_2\sqrt{k})}{(a_2{}^2-b_2{}^2k)} = \frac{(a_1a_2-b_1b_2k) + (a_2b_1-a_1b_2)\sqrt{k}}{(a_2{}^2-b_2{}^2k)} = \frac{(a_1a_2-b_1b_2k)}{(a_2{}^2-b_2{}^2k)} + \frac{(a_2b_1-a_1b_2)}{(a_2{}^2-b_2{}^2k)}\sqrt{k}\ .$$

However, for the sake of this exploration, we are only interested in integers, i.e. when $\frac{(a_1a_2-b_1b_2k)}{(a_2{}^2-b_2{}^2k)}, \frac{(a_2b_1-a_1b_2)}{(a_2{}^2-b_2{}^2k)}\ \epsilon\ \mathbb{Z}$; when these former two expressions are integers, it gives rise to factors of $a_1 + b_1\sqrt{k}$ that are also numbers in the same form. Let us call these numbers the irrational divisors or IDs.

Finding the IDs

Let us say the number we want to find the IDs of $m + n\sqrt{k}$. By definition, $\frac{(m+n\sqrt{k})}{(a_2+b_2\sqrt{k})} = \left(a_1 + b_1\sqrt{k}\right)$, so $\left(m + n\sqrt{k}\right) = \left(a_2 + b_2\sqrt{k}\right)\left(a_1 + b_1\sqrt{k}\right) = (a_1a_2 + b_1b_2k) + (a_1b_2 + a_2b_1)\sqrt{k}$. If we compare coefficients, we obtain 1.1 and 1.2.

$$a_1a_2 + kb_1b_2 = m \quad (1.1)$$
$$a_1b_2 + a_2b_1 = n \quad (1.2)$$

These 2 equations represent a system of linear Diophantine equations. One possible way to solve this system of these equations would be to use trial-and-error, but it would be very inefficient, since we would have to then go through every possible combination for a_1, a_2, b_1, and b_2 to find possible solutions. Finding a general solution for this system of linear Diophantine equations (i.e. finding a general solution for all the IDs of $m + n\sqrt{k}$) requires field theory, which is beyond the level of mathematics in this exploration. Nonetheless, as it is too hard to solve these equations, we could perhaps ask a simpler question, namely when k specified. Thus, let us examine the simplest case where k = 2 (i.e. $m + n\sqrt{2}$). We want to know whether $m + n\sqrt{2}$ can always be factorised, and to determine this, we need to familiarise ourselves with the concept of the norm.

For a number $m+n\sqrt{2}$, we define its norm to be $\mathrm{N}(m+n\sqrt{2})=(m+n\sqrt{2})(m-n\sqrt{2})=m^2-2n^2 \in \mathbb{Z}$. If $\mathrm{X}=a+b\sqrt{2}$ and $\mathrm{Y}=c+d\sqrt{2}$, then we can verify that N(XY) = N(X)N(Y), which is known as the multiplicative property, since as $\mathrm{N(XY)}=(ac+2bd)^2-\left((ad+bc)\sqrt{2}\right)^2=a^2c^2+4b^2d^2-2a^2d^2-2b^2c^2=(a^2-2b^2)(c^2-2d^2)=\mathrm{N(X)N(Y)}$ (Cornell University). Moreover, when N(X) = ±1, we call X a unit (analogous to 1 in the set of positive integers).

Therefore, let us first look at the case when N(X) = ±1, i.e. when $a^2-2b^2=\pm1$. If X = PQ, then N(PQ) = N(P)N(Q) = ±1, so N(P) = ±1 and N(Q) = ±1. This means that all the pair of integer solutions (t,s) to the equation $a^2-2b^2=\pm1$ form a number $t+s\sqrt{2}$ that consists of IDs whose integer term and coefficient of $\sqrt{2}$ also satisfy the same equation. Because $a^2-2b^2=\pm1$ is a Pell's equation that has infinite integer solutions (The IMO Compendium Group, 2007), $t+s\sqrt{2}$ must have an infinite number of IDs. E.g., for the case when $a^2-2b^2=1$, a few solutions are (1,1), (3,2), and (7,5). Therefore, if we want to find the IDs of $1+\sqrt{2}$ for example, we know it has infinite IDs. If we test this out for a few factors using the solutions (3,2), and (7,5), we see that $\frac{(1+\sqrt{2})}{(3+2\sqrt{2})}=(-1+\sqrt{2})$ and $\frac{(1+\sqrt{2})}{(7+5\sqrt{2})}=(3-2\sqrt{2})$, which are indeed numbers in the desired form.

Another case would be when N(X) = ±j, where j ≥ 2, i.e. $a^2-2b^2=\pm\mathrm{j}$

1. If j is prime then, without loss of generality, N(P) = ±1 and N(Q) = ±j. By finding solutions to $a^2-2b^2=\pm\mathrm{j}$ or ±1 and forming a number in the same form, we could determine the IDs of the original number; by dividing the original number by its IDs, other IDs could be determined.
2. If j is composite then, without loss of generality, $\mathrm{N(P)}=\pm f_1$ and $\mathrm{N(Q)}=\pm f_2$, where f_1 and f_2 are two arbitrary factors. Like above, by finding solutions to $a^2-2b^2=\pm f_1$ or $\pm f_2$ and forming a number in the same form, we could determine the IDs of the original number; by dividing the original number by its IDs, other factors could be formed. Nonetheless, it is important to note that $a^2-2b^2=\pm f_1$ or $\pm f_2$ does not always has integer solutions, as some Pell-type equations such $a^2-2b^2=10$ do not have integer solutions (this was verified using Wolfram Alpha).

For instance, if j = 3, then we need to find solutions to $a^2-2b^2=\pm3$ or ±1. Let us look at $a^2-2b^2=\pm3$ (since we have already looked at $a^2-2b^2=\pm1$). A few solutions of this Pell-type equation are (1,-1), (17,-12), and (41,-29). Therefore, $1-\sqrt{2}$ has infinite IDs, including $17-12\sqrt{2}$ and $41-29\sqrt{2}$, as $\frac{(1-\sqrt{2})}{(17-12\sqrt{2})}=(-7-5\sqrt{2})$ and $\frac{(1+\sqrt{2})}{(41-29\sqrt{2})}=(17+12\sqrt{2})$, which are indeed numbers in the desired form.

Moreover, from our observations above, we now know that the number $m+n\sqrt{2}$ does not necessarily have factors, meaning that the set of numbers in the form $m+n\sqrt{2}$ is not closed under division. If we extend these observations, it is likely that the set of numbers in the form $m+n\sqrt{k}$ is also not closed under division, but we cannot be certain about this assertion, since we have not proved this.

2.3 – Positive integer powers of $a+b\sqrt{k}$

Let us say that $\left(a+b\sqrt{k}\right)^n=a_n+b_n\sqrt{k}$, where n is a positive integer. If we take the binomial expansion of $\left(a+b\sqrt{k}\right)^n$, the result is quite remarkable because we always obtain a number in the same form:

If n is odd:

$$\left(a+b\sqrt{k}\right)^n=\binom{n}{0}a^n+\binom{n}{1}a^{n-1}\left(b\sqrt{k}\right)+\binom{n}{2}a^{n-2}\left(b\sqrt{k}\right)^2+\ldots+\binom{n}{n-1}a\left(b\sqrt{k}\right)^{n-1}+\binom{n}{n}\left(b\sqrt{k}\right)^n=$$
$$\left(a^n+\left(\frac{n(n-1)}{2!}\right)a^{n-2}kb^2+\ldots+\left(\frac{n(n-1)}{2!}\right)ab^{n-1}k^{\frac{1}{2}n-\frac{1}{2}}\right)+\left(na^{n-1}b+\cdots+b^nk^{\frac{1}{2}n-\frac{1}{2}}\right)\sqrt{k}$$

If n is even:

$$\left(a^n+\left(\frac{n(n-1)}{2!}\right)a^{n-2}kb^2+\ldots+b^nk^{\frac{n}{2}}\right)+\left(na^{n-1}b+\cdots+\left(\frac{n(n-1)}{2!}\right)ab^{n-1}k^{\frac{1}{2}n-\frac{1}{4}}\right)\sqrt{k}$$

By inspection, as $a, b, k, n \in \mathbb{Z}$, we can say the set of numbers in the form $m + n\sqrt{k}$ is closed under exponentiation (where the exponent is a positive integer). Let us carry out an example. If a = 1, b = 1, k = 2, and n = 3, $\left(1+\sqrt{2}\right)^3 = 1 + 3\sqrt{2} + 6 + 2\sqrt{2} = 7 + 5\sqrt{2}$, which is indeed a number in the same form.

Observations

Expanding $\left(a + b\sqrt{k}\right)^n$ using the binomial theorem is one method for finding the values a_n and b_n. However, what if we want to directly relate the values a_n and b_n to a and b? If we make some further observations, we can find recurrence relations for the values a_n and b_n.

Figure 1.1 – A table to show the observations of $\left(a + b\sqrt{k}\right)^n$

$a_1 + b_1\sqrt{k}$	n	$\left(a_1 + b_1\sqrt{k}\right)^n$	a_n	b_n	Minimal polynomial ($\alpha_n x^2 + \beta_n x + \gamma_n$)	α_n	β_n	γ_n
$1+\sqrt{2}$	1	$1+\sqrt{2}$	1	1	x^2-2x-1	1	-2	-1
	2	$3+2\sqrt{2}$	3	2	x^2-6x+1	1	-6	1
	3	$7+5\sqrt{2}$	7	5	$x^2-14x-1$	1	-14	-1
	…	…	…	…	…	…	…	…
	n	$(a_{n-1}+2b_{n-1})+(a_{n-1}+b_{n-1})\sqrt{2}$	$a_{n-1}+2b_{n-1}$	$a_{n-1}+b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$2+\sqrt{2}$	1	$2+\sqrt{2}$	2	2	x^2-4x+1	1	-4	1
	2	$6+4\sqrt{2}$	6	4	$x^2-12x+1$	1	-12	1
	3	$20+14\sqrt{2}$	20	14	$x^2-40x+1$	1	-40	1
	…	…	…	…	…	…	…	…
	n	$(2a_{n-1}+2b_{n-1})+(a_{n-1}+2b_{n-1})\sqrt{2}$	$2a_{n-1}+2b_{n-1}$	$a_{n-1}+2b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$3+\sqrt{2}$	1	$3+\sqrt{2}$	3	1	x^2-6x+7	1	-6	7
	2	$11+6\sqrt{2}$	11	6	$x^2-22x+49$	1	-22	49
	3	$45+29\sqrt{2}$	45	29	$x^2-90x+343$	1	-90	343
	…	…	…	…	…	…	…	…
	n	$(3a_{n-1}+2b_{n-1})+(a_{n-1}+3b_{n-1})\sqrt{2}$	$3a_{n-1}+2b_{n-1}$	$a_{n-1}+3b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$1+2\sqrt{2}$	1	$1+2\sqrt{2}$	1	2	x^2-2x-7	1	-2	-7
	2	$9+4\sqrt{2}$	9	4	$x^2-18x+49$	1	-18	49
	3	$25+22\sqrt{2}$	25	22	$x^2-50x+343$	1	-50	343
	…	…	…	…	…	…	…	…
	n	$(a_{n-1}+4b_{n-1})+(2a_{n-1}+b_{n-1})\sqrt{2}$	$a_{n-1}+4b_{n-1}$	$2a_{n-1}+b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$2+2\sqrt{2}$	1	$2+2\sqrt{2}$	2	2	x^2-4x+7	1	-4	7
	2	$12+8\sqrt{2}$	12	8	$x^2-24x+49$	1	-24	49
	3	$56+40\sqrt{2}$	56	40	$x^2-112x+343$	1	-112	343
	…	…	…	…	…	…	…	…
	n	$(2a_{n-1}+4b_{n-1})+(2a_{n-1}+2b_{n-1})\sqrt{2}$	$2a_{n-1}+4b_{n-1}$	$2a_{n-1}+2b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$3+2\sqrt{2}$	1	$3+2\sqrt{2}$	3	2	x^2-6x+1	1	-6	1
	2	$17+12\sqrt{2}$	17	12	$x^2-34x+1$	1	-36	1
	3	$99+70\sqrt{2}$	99	70	$x^2-198x+343$	1	-198	1
	…	…	…	…	…	…	…	…
	n	$(3a_{n-1}+4b_{n-1})+(2a_{n-1}+3b_{n-1})\sqrt{2}$	$3a_{n-1}+4b_{n-1}$	$2a_{n-1}+3b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$1+3\sqrt{2}$	1	$1+3\sqrt{2}$	1	3	$x^2-2x-17$	1	-2	-17
	2	$19+6\sqrt{2}$	19	6	$x^2-38x+289$	1	-38	289
	3	$55+63\sqrt{2}$	55	63	$x^2-110x+4913$	1	-110	4913
	…	…	…	…	…	…	…	…
	n	$(a_{n-1}+6b_{n-1})+(3a_{n-1}+b_{n-1})\sqrt{2}$	$a_{n-1}+6b_{n-1}$	$3a_{n-1}+b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$2+3\sqrt{2}$	1	$2+3\sqrt{2}$	2	3	$x^2-4x-14$	1	-4	-14
	2	$22+12\sqrt{2}$	22	12	$x^2-44x+196$	1	-44	196
	3	$116+90\sqrt{2}$	116	90	$x^2-232x-2744$	1	-232	-2744
	…	…	…	…	…	…	…	…
	n	$(2a_{n-1}+6b_{n-1})+(3a_{n-1}+2b_{n-1})\sqrt{2}$	$2a_{n-1}+6b_{n-1}$	$3a_{n-1}+2b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
….	…	…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…

We can clearly now see a pattern for both the values for a_n and b_n, as $a_n = a_1a_{n-1} + 2b_1b_{n-1}$ and $b_n = b_1a_{n-1} + a_1b_{n-1}$, but we cannot assume that this is true for other numbers where k is different, and/or a and/or b are negative. So, we have to continue making observations for different values and signs.

<u>Figure 1.1 (continued)</u>

$a_1+b_1\sqrt{k}$	n	$\left(a_1+b_1\sqrt{k}\right)^n$	a_n	b_n	Minimal polynomial $(\alpha_n x^2+\beta_n x+\gamma_n)$	α_n	β_n	γ_n
$1+\sqrt{3}$	1	$1+\sqrt{3}$	1	1	x^2-2x-2	1	-2	-2
	2	$4+2\sqrt{3}$	4	2	x^2-8x+4	1	-8	4
	3	$10+6\sqrt{3}$	10	6	$x^2-20x-8$	1	-20	-8
	...	...	...	...	...	...	...	...
	n	$(a_{n-1}+3b_{n-1})+(a_{n-1}+b_{n-1})\sqrt{3}$	$a_{n-1}+3b_{n-1}$	$a_{n-1}+b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$2+\sqrt{3}$	1	$2+\sqrt{3}$	2	1	x^2-4x+1	1	-4	1
	2	$7+4\sqrt{3}$	7	4	$x^2-14x+1$	1	-14	1
	3	$26+15\sqrt{3}$	26	15	$x^2-52x+1$	1	-52	1
	...	...	...	...	...	...	...	...
	n	$(2a_{n-1}+3b_{n-1})+(a_{n-1}+2b_{n-1})\sqrt{3}$	$2a_{n-1}+3b_{n-1}$	$a_{n-1}+2b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$1+2\sqrt{3}$	1	$1+2\sqrt{3}$	1	2	$x^2-2x-11$	1	-2	-11
	2	$13+4\sqrt{3}$	13	4	$x^2-26x+121$	1	-26	121
	3	$37+30\sqrt{3}$	37	30	$x^2-74x-1331$	1	-74	-1331
	...	...	...	...	...	...	...	...
	n	$(a_{n-1}+6b_{n-1})+(2a_{n-1}+b_{n-1})\sqrt{3}$	$a_{n-1}+6b_{n-1}$	$2a_{n-1}+b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$2+2\sqrt{3}$	1	$2+2\sqrt{3}$	2	2	x^2-4x-8	1	-4	-8
	2	$16+8\sqrt{3}$	16	8	$x^2-32x+64$	1	-32	64
	3	$80+48\sqrt{3}$	80	48	$x^2-160x-512$	1	-160	-512
	...	...	...	...	...	...	...	...
	n	$(2a_{n-1}+6b_{n-1})+(2a_{n-1}+2b_{n-1})\sqrt{3}$	$2a_{n-1}+6b_{n-1}$	$2a_{n-1}+2b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
$1+3\sqrt{3}$	1	$1+3\sqrt{3}$	1	3	$x^2-2x-26$	1	-4	-26
	2	$28+6\sqrt{3}$	28	6	$x^2-56x+676$	1	-56	676
	3	$82+90\sqrt{3}$	82	90	$x^2-164x-17576$	1	-164	−17576
	...	...	...	...	...	...	...	...
	n	$(a_{n-1}+9b_{n-1})+(3a_{n-1}+b_{n-1})\sqrt{3}$	$a_{n-1}+9b_{n-1}$	$3a_{n-1}+b_{n-1}$	$x^2-2a_nx+\gamma_1^n$	1	$-2a_n$	γ_1^n
...	...	...	...	...	...	...	...	
...	...	...	...	...	...	...	...	

From Figure 1.1, we realise we can modify our recurrence relation for a_n (the table also shows that the recurrence relation for b_n stays the same, since it is independent of the value of k) to $a_n = a_1a_{n-1} + kb_1b_{n-1}$. For example, suppose we want to find the values a_4 and b_4 of $\left(15+9\sqrt{11}\right)^4 = a_4 + b_n\sqrt{11}$. If we know a_3 and b_3, we should be able to calculate a_4 and b_4 using the recurrence relations for a_n and b_n. $a_3 = 43470$ and $b_3 = 14094$, so $a_4 = 15 \times 43470 + 11 \times 9 \times 14094 = 2{,}047{,}356$ and $b_4 = 15 \times 14094 + 9 \times 43470 = 602640$, which are indeed the values for a_4 and b_4 of $\left(15+9\sqrt{11}\right)^4$.

If we carry out the same process for a and/or b being a negative integer, we can figure out the recurrence relations for 4 general cases, which are in fact the same:

	$b_1 \epsilon\, \mathbb{Z}^+$	$b_1 \epsilon\, \mathbb{Z}^-$
$a_1 \epsilon\, \mathbb{Z}^+$	$a_n = a_1a_{n-1} + kb_1b_{n-1}$	
$a_1 \epsilon\, \mathbb{Z}^-$	$b_n = b_1a_{n-1} + a_1b_{n-1}$	

<u>Proving these recursions using induction</u>

These recurrences are based on mere observation, so in order to completely validate them we must prove them. One way to do this is by using proof by induction:

1. Let us call the statements $a_n = a_1a_{n-1} + kb_1b_{n-1}$ and $b_n = b_1a_{n-1} + a_1b_{n-1}$ A(n) and B(n) respectively.
2. Let $a_1 = s$ and $b_1 = t$, i.e. consider the number $s + t\sqrt{k}$.

<u>Base Case:</u>

For n = 2, $\left(s+t\sqrt{k}\right)^2 = (s^2+kt^2) + (2st)\sqrt{k}$, so $a_2 = s^2 + kt^2$ and $b_2 = 2st$
Also, $a_2 = s \times s + kt \times t = s^2 + kt^2$ and $b_2 = t \times s + s \times t = 2st$

Therefore, A(n) and B(n) are true for n=2.

Inductive Step:
Assume that A(n) and B(n) are true for n=m:

$$a_m = a_1 a_{m-1} + k b_1 b_{m-1} \text{ and } b_m = b_1 a_{m-1} + a_1 b_{m-1}.$$

We are required to prove that if A(n) and B(n) are true for n=m, then A(n) and B(n) are true for n=m+1. Thus, we are working towards:

$$a_{m+1} = a_1 a_m + k b_1 b_m \text{ and } b_{m+1} = b_1 a_m + a_1 b_m.$$

We know that $\left(s + t\sqrt{k}\right)^m = a_m + b_m\sqrt{k}$. So,

$$\left(s + t\sqrt{k}\right)^{m+1} = \left(s + t\sqrt{k}\right)^m \left(s + t\sqrt{k}\right) = \left(a_m + b_m\sqrt{k}\right)\left(s + t\sqrt{k}\right) = (s a_m + k t b_m) + (t a_m + s b_m)\sqrt{k}.$$
$$a_{m+1} = s a_m + k t b_m = a_1 a_m + k b_1 b_m \text{ and } b_{m+1} = t a_m + s b_m = b_1 a_m + a_1 b_m.$$

Therefore, A(m+1) and B(m+1) are true.

Henceforth, by the principle of mathematical induction, if A(n) and B(n) are true, then A(n+1) and B(n+1) are also true, and because A(2) and B(2) are true, A(n) and B(n) are true for all $n \geq 2$.

Solving simultaneous recurrence relations.
Now that we have proved that A(n) and B(n) are true for all $n \geq 2$ (A(1) and B(1) are given), we can solve them simultaneously, as we have a system of two linear first order recurrence relations. Solving these recurrence relations, we obtain to the following solutions:

$$a_n = \frac{\left(a_1 + b_1\sqrt{k}\right)^n + \left(a_1 - b_1\sqrt{k}\right)^n}{2}$$
$$b_n = \frac{\left(a_1 + b_1\sqrt{k}\right)^n - \left(a_1 - b_1\sqrt{k}\right)^n}{2\sqrt{k}}$$

Let us carry out an example where we want to find $\left(5 + 5\sqrt{7}\right)^5$. From the solutions above:

$$a_5 = \frac{\left(5+5\sqrt{7}\right)^5 + \left(5-5\sqrt{7}\right)^5}{2} = 987500$$

$$b_5 = \frac{\left(5+5\sqrt{7}\right)^5 - \left(5-5\sqrt{7}\right)^5}{2\sqrt{7}} = 387500,$$

which are indeed the values for a_5 and b_5 for $\left(5 + 5\sqrt{7}\right)^5$.

By looking at these solutions for the recurrence relations, we realise that they make sense, since a_n eliminates all the irrational terms (including $\sqrt{7}$) and divides through by 2, since the rational numbers are doubled. Similarly, b_n eliminates all the rational terms and divides through by $2\sqrt{7}$ since the irrational numbers are doubled and b_n does not include $\sqrt{7}$. As mathematicians, we are relieved as we can corroborate that the binomial expansion is the fastest way to calculate $\left(a + b\sqrt{k}\right)^n$ - the solutions for the recurrence relations for a_n and b_n themselves include two terms in the form $\left(a + b\sqrt{k}\right)^n$, which means that it takes exponentially more time to find a_n and b_n relative to using binomial expansion.

2.4 – The minimal polynomial of $a + b\sqrt{k}$

The last four columns of Figure 1.1 show the minimal polynomial of $a + b\sqrt{k}$, which is the unique, lowest degree polynomial with integer coefficients (including the term independent of the variable) that has $a + b\sqrt{k}$ as one of its roots. Additionally, the coefficient of the highest degree term is required to be 1.

The first observation I made from Figure 1.1 was that all the coefficients of the all the terms of $\alpha_n x^2 + \beta_n x + \gamma_n$ were integers. Also, for every single observation, the minimal polynomial of $\left(a + b\sqrt{k}\right)^n = a_n + b_n\sqrt{k}$ was $x^2 - 2a_n x + \gamma_1^n$, where γ_1 is the constant term of the minimal polynomial of $a_1 + b_1\sqrt{k}$. We can prove these observations using the quadratic formula and comparing coefficients:

<u>Proving these observations</u>
The quadratic formula is:

$$x = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}$$

In our case $\alpha = 1$ (by definition) and x $= a \pm b\sqrt{k}$. So, by substitution,

$$a \pm b\sqrt{k} = \frac{-\beta \pm \sqrt{\beta^2 - 4\gamma}}{2} = \frac{-\beta}{2} \pm \frac{1}{2}\sqrt{\beta^2 - 4\gamma}$$

Comparing coefficients, we obtain:

$$a = \frac{-\beta}{2} \text{ and } b\sqrt{k} = \frac{1}{2}\sqrt{\beta^2 - 4\gamma}$$

Then, solving for β, we obtain:

$$\beta = -2a \ (\beta_n = -2a_n)$$

Also, solving for γ, we obtain:

$$2b\sqrt{k} = \sqrt{\beta^2 - 4\gamma}$$
$$4b^2k = \beta^2 - 4\gamma$$
$$4b^2k = (-2a)^2 - 4\gamma$$
$$4\gamma = 4a^2 - 4b^2k$$
$$\gamma = a^2 - b^2k \ (\gamma_n = a_n^2 - kb_n^2)$$

However, in my observation we saw that $\gamma_n = \gamma_1^n$. So, either my observation is incorrect or both of them are equivalent. So, let us try to prove that both of them are identical.

$$\gamma_1^n = (a_1^2 - kb_1^2)^n = \left[\left(a_1 + b_1\sqrt{k}\right)\left(a_1 - b_1\sqrt{k}\right)\right]^n = \left(a_1 + b_1\sqrt{k}\right)^n\left(a_1 - b_1\sqrt{k}\right)^n = \left(a_n + b_n\sqrt{k}\right)\left(a_n - b_n\sqrt{k}\right) = a_n^2 - kb_n^2 = \gamma_n$$

Therefore, we have proved γ_1^n and γ_n are interchangeable expressions, meaning that $x^2 - 2a_n + \gamma_1^n = x^2 - 2a_n + (a_n^2 - kb_n^2)$ is a valid expression for the minimal polynomial of $a_n + b_n\sqrt{k}$.

Also, since $a_n, b_n \epsilon\ \mathbb{Z}$, $-2a_n, a_n^2 - kb_n^2 \epsilon\ \mathbb{Z}$, so all the coefficients of the all the terms of $\alpha_n x^2 + \beta_n x + \gamma_n$ must be integers, which explains the first observation I made. From deduction, we also see that the converse is true (i.e. if the minimal polynomial has integer coefficients, $a_n, b_n \epsilon\ \mathbb{Z}$).

<u>2.5 – Negative integer powers of $a + b\sqrt{k}$</u>
While $a + b\sqrt{k}$ raised to a positive integer power always guarantees a number in the desired form (i.e. when a_n and b_n are integer values), $\left(a + b\sqrt{k}\right)^{-n}$, where $n \ \epsilon\ \mathbb{Z}^+$, does not necessarily do the same.

$\left(a+b\sqrt{k}\right)^{-n} = \frac{1}{\left(a+b\sqrt{k}\right)^{n}} = \frac{1}{a_n+b_n\sqrt{k}} = \frac{a_n-b_n\sqrt{k}}{(a_n+b_n\sqrt{k})(a_n-b_n\sqrt{k})} = \frac{a_n-b_n\sqrt{k}}{a_n^2-kb_n^2} = \frac{a_n}{a_n^2-kb_n^2} - \frac{b_n}{a_n^2-kb_n^2}\sqrt{k}$ and $\frac{a_n}{a_n^2-kb_n^2}, \frac{-b_n}{a_n^2-kb_n^2}$ are not always integers. This is quite an interesting problem, but we can actually solve this problem by using certain properties of minimal polynomials that we investigated above (which is why I have put this section after Part 2.5 and not Part 2.4).

From Part 2.4, we have proved that the number $\left(a+b\sqrt{k}\right)^{n}$ is the root of $x^2-\beta_n x+\gamma_n = 0$ (where $\beta_n, \gamma_n \epsilon\, \mathbb{Z}$). As we know that $\left(a+b\sqrt{k}\right)^{-n} = \frac{1}{\left(a+b\sqrt{k}\right)^{n}}$, we can deduce that this number is the root of $\left(\frac{1}{x}\right)^2-\beta_n\left(\frac{1}{x}\right)+\gamma_n = 0$, which is equivalent to $x^2-\frac{\beta_n}{\gamma_n}x+\frac{1}{\gamma_n} = 0$. We know that if $a, b\epsilon\, \mathbb{Z}$, the minimal polynomial must have integer coefficients (the converse is also true), implying that γ_n must divide β_n and 1. Therefore, by inspection, we can see that the only possible values for γ_n can be ± 1. However, since $\gamma_1^n = \gamma_n$, $\gamma_1^n = \pm 1$, so $\gamma_1 = \pm 1$. Therefore, as $\gamma_1 = a_1^2-kb_1^2$, whenever $a_1^2-kb_1^2 = \pm 1$, $a_n^2-kb_n^2 = \pm 1$ and $\left(a+b\sqrt{k}\right)^{-n}$ equals a number in the desired form for all $n \,\epsilon\, \mathbb{Z}^+$.

Coincidently, $a_1^2-kb_1^2 = \pm 1$ is Pell's equation, which we have already met above. Nonetheless, solving this equation using methods such as continued fractions are beyond the scope of this exploration, so for now I will just state the smallest integer solutions or the fundamental solutions to Pell's equation for $k \leq 10$.

Figure 1.2a – A table to show the fundamental solutions for $a_1^2-kb_1^2 = 1$

k	a_1	b_1
1	-	-
2	± 3	± 2
3	± 2	± 1
4	-	-
5	± 9	± 4
6	± 5	± 2
7	± 8	± 3
8	± 3	± 1
9	-	-
10	± 19	± 6

Figure 1.2b – A table to show the fundamental solutions for $a_1^2-kb_1^2 = -1$

k	a_1	b_1
1	-	-
2	± 1	± 1
3	-	-
4	-	-
5	± 2	± 1
6	-	-
7	-	-
8	-	-
9	-	-
10	± 3	± 1

Therefore, if we take a random number $m + n\sqrt{k}$ and raise it to a negative integer power, it will either never be a number in the desired form or always be a number in the desired form, depending on whether $m^2 - kn^2 = \pm 1$. For example, if we take $15 + 22\sqrt{6}$, $15^2 - 6 \times 22^2 = -2679 \neq \pm 1$, meaning that if we take $\left(15 + 22\sqrt{6}\right)^{-n}$, it will never equal a number in the desired form. However, if we take $19 + 6\sqrt{10}$ on the other hand, $19^2 - 10 \times 6^2 = 1$, implying that $\left(19 + 6\sqrt{10}\right)^{-n}$, it will always equal a number in the desired form. E.g. for n = 7, $\left(19 + 6\sqrt{10}\right)^{-7} = 56830852179 - 18003116202\sqrt{10}$ which is indeed a number $m + n\sqrt{k}$, where m and n are non-zero integers.

Moreover, we can also conclude that $m + n\sqrt{k}$ is closed under exponentiation (where the exponent is a negative integer) if and only if $m^2 - kn^2 = \pm 1$ has integer solutions.

3.1 – Applications of the observations made

Although it may seem unlikely at first, certain properties of $a + b\sqrt{k}$ have practical purposes. Proving that we only obtain numbers in the desired form for $\left(a + b\sqrt{k}\right)^{-n}$ when Pell's equation is satisfied can clearly be applied to show the infinite nature of the integer solutions. In other words, there exists a bijection between the solutions to the problem I attempted to solve in Part 2.5 and the solutions of Pell's equation, which is quite beautiful because it also elucidates an intuitive way in which one can generate all the integers solutions to Pell's equation!

Additionally, the set of numbers in form $a + b\sqrt{k}$ is closed linked to group theory as well. Even though numbers in the form $a + b\sqrt{k}$ appear similar superficially, understanding that this set of numbers do not form groups and rings under the basic operations and exponentiation allows mathematicians to comprehend the asymmetry that also exists between them.

3.2 – Conclusion

Finding subtle relationships between different numbers of this same form is an epitome of the connection, beauty, and mystery that lies within number theory and mathematics. Moreover, this essay has shed light upon the fact that any recognisable pattern can generally be explained using mathematics.

To my fellow mathematicians, I hope further questions are asked. Do these numbers act similarly if we take any nth root? What if we extend the realm of these numbers to the real and complex plane? What happens when k is a non-square negative integer, and when a and b are complex numbers? Are there any more fascinating links? The questions that can be asked are uncountably infinite…

4.1 – Acknowledgements

Dr Tom Crawford and The University of Oxford for providing me with the opportunity to share my love for mathematics!

4.2 – Bibliography

Conrad, K. (n.d.). *THE MINIMAL POLYNOMIAL AND SOME APPLICATIONS.* Retrieved July 15, 2018, from http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/minpolyandappns.pdf

Cornell University. (n.d.). *Quadratic Fields.* Retrieved August 19, 2018, from http://pi.math.cornell.edu/~hatcher/3320/TNch3.pdf

Hayes, A. (n.d.). *Linear Diophantine Equations.* Retrieved July 13, 2018, from https://brilliant.org/wiki/linear-diophantine-equations-one-equation/

Illinois University. (n.d.). *Fundamental Mathematics - 347 G1.* Retrieved July 13, 2018, from https://faculty.math.illinois.edu/~rdeville/teaching/347/hw6S.pdf

James Madison University . (2000). Retrieved July 13, 2018, from http://educ.jmu.edu/~taalmala/235_2000post/235contradiction.pdf

MathBitsNotebook. (n.d.). *Sum/Product - Rationals and Irrationals.* Retrieved July 13, 2018, from https://mathbitsnotebook.com/Algebra1/RatIrratNumbers/RNRationalIrrationalSumProduct.html

William J. Gilbert, A. P. (1990). *Linear Diophantine Equations.* Retrieved July 13, 2018, from https://www.math.uwaterloo.ca/~wgilbert/Research/GilbertPathria.pdf