Integer difference of powers

L. Castillo

Abstract

I explore a method to characterize all the real numbers a, b such that all of $a - b, a^2 - b^2, ..., a^n - b^n$ are integers for a given n and paying particular attention to the special case when neither of a and b are integers themselves.

Keywords: Elementary Number Theory

1. Motivation

It is a known property [1] that if $a, b \in \mathbb{R}, a \neq b$ and $\forall n \in \mathbb{N}, a^n - b^n \in \mathbb{Z}$ then necessarily $a, b \in \mathbb{Z}$. What is interesting about this fact is that it is provable by contradiction, without needing much insight into what kind of numbers satisfy an incomplete part of the hypothesis. For example, it is not necessary to know what kind of numbers satisfy the property up to $n = 4$. However, when studying this partial version of the theorem an interesting structure arises. In this paper I find the form of the numbers that satisfy this property for $n = 2, 3, 4$ with methods that can be easily extended to find the forms of numbers that satisfy this property for larger n. For this I present the dollowing definition:

Definition .1. The pair $(a, b) \in \mathbb{R}^2, a \neq b$ is said to be an integer point of degree n if and only if $a^k - b^k \in \mathbb{Z}$ for all $k \in \{1, 2, 3, ..., n\}$

And I will say the pair is a non-trivial integer point of degree n if and only if $a, b \notin \mathbb{Z}$

The case n=1 is trivial so for this paper I consider $n > 1$.

2. The existence of non-trivial integer points of arbitrarily large degree

A normal question that arises from this study is whether there exists a biggest n such that no non-trivial integer points exist with degree larger than n. The following theorem shows that there is no such limit:

Theorem 1. There exist non-trivial integer points of arbitrarily large degree

Proof. Let $n \in \mathbb{N}$. Now consider the point $\left(\frac{1}{2}, 2^n + \frac{1}{2}\right)$. Considering the expansion of $\left(2^n + \frac{1}{2}\right)^k$ given by the binomial theorem, the first term will be of the form $(2^n)^k$ and the last term will be of the form $\left(\frac{1}{2}\right)^k$ and the intermediate terms are of the form $m(2^n)^i \left(\frac{1}{2}\right)^j$. As in this intermediate terms $i \geq 1$ and $j \leq n - 1$, these intermediate terms will always

be integers and therefore the fractional part of $\left(2^n + \frac{1}{2}\right)^k$ will be exactly $\left(\frac{1}{2}\right)^k$ and thus the fractional parts will be cancelled in the subtraction, leaving an integer. Thus, this point will be an integer point of degree n. As I can choose n arbitrarily big, the theorem is proved. □

The previous theorem shows that there are many interesting rational numbers out there. However, coming up with special examples like the one used is trivial so what is of interest is characterizing all the integer points of a certain degree with a generating expression.

3. Integer points of second degree

Integer points of second degree have a neat geometric structure and to show it consider the following theorem:

Theorem 2. (a, b) is a second degree integer point if and only if it is of the form $\left(\frac{k}{2c}, \frac{k}{2c} + c\right)$ with $k, c \in \mathbb{Z}$.

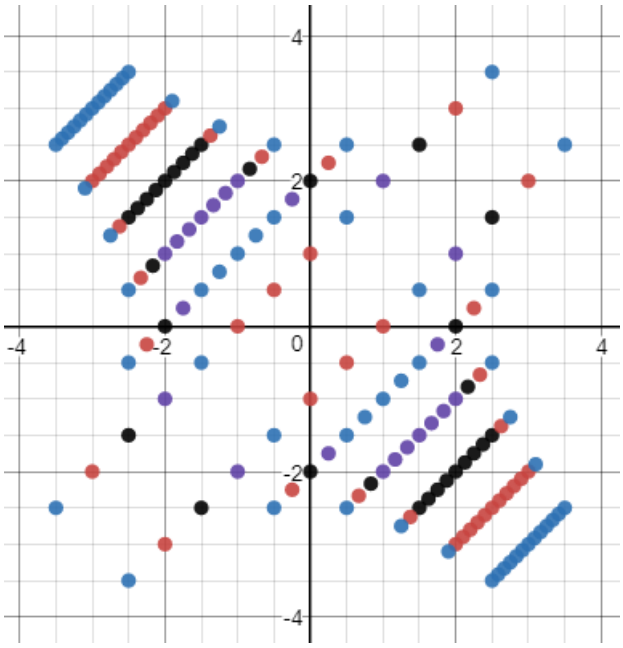
Proof. Suppose that $a - b = n \in \mathbb{Z}$ and $a^2 - b^2 = m \in \mathbb{Z}$. By the difference of squares formula, $(a - b)(a + b) = m$ and therefore $a + b = \frac{m}{n}$.

Adding the equations for $a - b$ and $a + b$ together we get that $2a = \frac{m}{n} + n = \frac{m+n^2}{n}$ and therefore $a = \frac{m+n^2}{2n}$. Similarly $b = \frac{m-n^2}{2n}$. Therefore, all second degree integer points can be generated by $\left(\frac{m+n^2}{2n}, \frac{m-n^2}{2n}\right)$ with each pair of integers m, n generating a unique integer point.

Now consider the substitution $c = -n, k = -n^2 - m$. This yields the form $\left(\frac{k}{2c}, \frac{k}{2c} + c\right)$.

I will now show that this substitution is one-to-one. Suppose that $c = -n_0 = -n_1$ and that $k = -m_0 - n_0^2 = -m_1 - n_1^2$. Then $n_0 = n_1$ and therefore $n_0^2 = n_1^2$ which implies that also $m_1 = m_0$. □

What is interesting about this form is that it resembles the parametric form of the line $(x, x + c)$ so by choosing an specific c and letting k vary, one can generate all the second degree integer points in a certain line. And this form also reveals how, as $|c|$ grows, the density of integer points of second degree in its line grows:



The previos image shows thirteen second degree integer points in each of lines $y = x + c$ for $c \in \{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$. The same amount of points is shown for each line, but see that as the lines get away from the origin, these points are more densely packed.

4. Integer points of third degree

To find a generating form of third degree integer points I first apply the property that all third degree integer points are second degree integers. Given this, these points are also of the form $\left(\frac{k}{2c}, \frac{k}{2c} + c\right)$. But they also satisfy that $\left(\frac{k}{2c}\right)^3 - \left(\frac{k}{2c} + c\right)^3 = \frac{(-4c^4 - 6c^2k - 3k^2)}{(4c)}$ must be an integer. Therefore, these numbers satisfy the congruence:

$$-4c^4 - 6c^2k - 3k^2 \equiv 0 \mod 4c$$

Which can be reduced to

$$3k^2 + 2kc^2 \equiv 0 \mod 4c$$

To solve this congruence first suppose that $c = 2^\alpha 3^\beta \prod_{i=1}^{z} p_i^{a_i}$ where p_i are primes bigger than 3. By the chinese remainder theorem, the congruence can be split up. First consider

$$3k^2 + 2kc^2 \equiv 0 \mod 2^{\alpha+2}$$

If k is odd the resulting number will be odd and thus a perfect power of 2 will not divide it. So now consider even k. As k is even, $2kc^2 \equiv 0 \mod 2^{\alpha+2}$ so the congruence simplifies to

$$3k^2 \equiv 0 \mod 2^{\alpha+2}$$

And as 3 is relatively prime to 2, this reduces to simply

$$k^2 \equiv 0 \mod 2^{\alpha+2}$$

Which is true as long as

$$k \equiv 0 \mod 2^{\lceil \frac{\alpha+2}{2} \rceil}$$

Now considering the congruence for 3^β, k must satisfy the congruence

$$3k^2 + 2kc^2 \equiv 0 \mod 3^\beta$$

and as $c \equiv 0 \mod 3^\beta$ this simplifies to

$$3k^2 \equiv 0 \mod 3^\beta$$

And as long as $\beta \geq 1$ then this simplifies to

$$k^2 \equiv 0 \mod 3^{\beta-1}$$

Which is true as long as

$$k \equiv 0 \mod 3^{\lceil \frac{\beta-1}{2} \rceil}$$

Interestingly, this last congruences holds true even in the case when $\beta = 0$ because then notice that it says $k \equiv 0 \mod 3^0$ which is trivially true, so no special consideration needs to be done for the case $\beta = 0$.

Finally, k must satisfy the congruence

$$3k^2 + 2kc^2 \equiv 0 \mod p_i^{a_i}$$

As $c \equiv 0 \mod p_i^{a_i}$ and 3 is relatively prime with p_i this congruence reduces to

$$k^2 \equiv 0 \mod p_i^{a_i}$$

Which is true as long as

$$k \equiv 0 \mod p_i^{\lceil \frac{a_i}{2} \rceil}$$

This yields all the congruences that k must satisfy. By the chinese remainder theorem these are united giving the congruence

$$k \equiv 0 \mod 2^{\lceil \frac{\alpha+2}{2} \rceil} 3^{\lceil \frac{\beta-1}{2} \rceil} \prod_{i=1}^{z} p_i^{\lceil \frac{a_i}{2} \rceil}$$

So k is of the form

$$k = n \times 2^{\lceil \frac{\alpha+2}{2} \rceil} 3^{\lceil \frac{\beta-1}{2} \rceil} \prod_{i=1}^{z} p_i^{\lceil \frac{a_i}{2} \rceil}, n \in \mathbb{Z}$$

Applying this we can compute

$$\frac{k}{2c} = \frac{n \times 2^{\lceil \frac{\alpha+2}{2} \rceil} 3^{\lceil \frac{\beta-1}{2} \rceil} \prod_{i=1}^{z} p_i^{\lceil \frac{a_i}{2} \rceil}}{2^{\alpha+1} 3^\beta \prod_{i=1}^{z} p_i^{a_i}} = \frac{n}{2^{\alpha+1-\lceil \frac{\alpha+2}{2} \rceil} 3^{\beta-\lceil \frac{\beta-1}{2} \rceil} \prod_{i=1}^{z} p_i^{a_i-\lceil \frac{a_i}{2} \rceil}}$$

And by applying the following identities:

$$x - \lceil \frac{x}{2} \rceil = \lceil \frac{x-1}{2} \rceil$$
$$x + 1 - \lceil \frac{x+2}{2} \rceil = \lfloor \frac{x}{2} \rfloor$$
$$x - \lceil \frac{x-1}{2} \rceil = \lceil \frac{x}{2} \rceil$$

This last expression can be simplified to

$$\frac{n}{2^{\lfloor \frac{\alpha}{2} \rfloor} 3^{\lceil \frac{\beta}{2} \rceil} \prod_{i=1}^{z} p_i^{\lceil \frac{a_i - 1}{2} \rceil}}$$

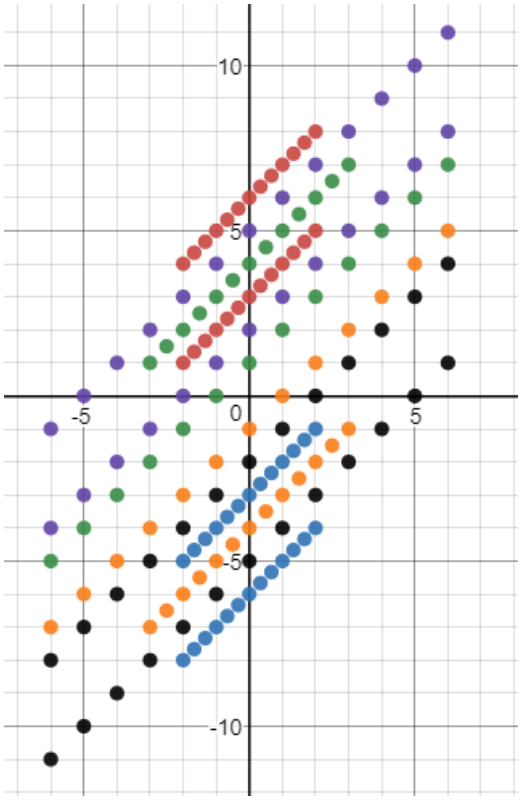
And this previous reasoning serves as proof of the next theorem

Theorem 3. (a,b) is a third degree point integer if and only if it is of the form

$$\left(\frac{\pm n}{2^{\lfloor \frac{\alpha}{2} \rfloor} 3^{\lceil \frac{\beta}{2} \rceil} \prod_{i=1}^{z} p_i^{\lceil \frac{a_i - 1}{2} \rceil}}, \frac{\pm n}{2^{\lfloor \frac{\alpha}{2} \rfloor} 3^{\lceil \frac{\beta}{2} \rceil} \prod_{i=1}^{z} p_i^{\lceil \frac{a_i - 1}{2} \rceil}} \pm 2^{\alpha} 3^{\beta} \prod_{i=1}^{z} p_i^{a_i} \right)$$

with $z, \alpha, \beta, a_i \in \mathbb{N}_0, n \in \mathbb{Z}$ and p_i arbitrary primes bigger than 3.

Using this generator formula one can find integer points of third degree in the plane:



Where a very different structure can be seen. The only lines with dense points are now $y = x \pm 3$, $y = x \pm 4$ and $y = \pm 6$. And yet, the points are not nearly as densely packed as they were in the image for second degree integer points.

This expression is much more complicated than the one for second degree integer points. This is because now the location of the points is highly dependent on the prime factorization of c. This can be reflected in the density of the points. While for the second degree points the density was only dependent on the magnitude of c, now it depends on how many different primes divide c, and how high the powers of these primes are. One of the first properties that can be found from the previous theorem is that if c is a square-free product of primes different from 3 then all the integer points in the corresponding line will be of the form $(n, n+c)$ so there won't be any non-trivial integer points in the line.

5. Integer points of degree 4

In this section I will prove a generating expression for all integer points of degree 4, while at the same time outlining how similar expressions may be found for integer points of higher degree. For simplicity, suppose that $\left(\frac{a}{b}, \frac{a}{b}+c\right)$ is a third degree integer point. To test if this point is also of fourth degree then it is necessary to show that $\left(\frac{a}{b}\right)^4 - \left(\frac{a}{b}+c\right)^4 = \frac{-(4a^3c)}{b^3} - \frac{(6a^2c^2)}{b^2} - \frac{(4ac^3)}{b} - c^4 \in \mathbb{Z}$

From Theorem 3, it can be decuded that b divides c and therefore all the terms are always integers, except for $\frac{-(4a^3c)}{b^3}$. So for this point to be of fourth degree, it is necessary that $4a^3c \equiv 0 \mod b^3$.

Replacing in this expression the corresponding terms found in theorem 3, choosing the positive form, it is necessary that

$$n^3 2^{\alpha+2} 3^{\beta} \prod_{i=1}^{z} p_i^{a_i} \equiv 0 \mod 2^{3\lfloor \frac{\alpha}{2} \rfloor} 3^{3\lceil \frac{\beta}{2} \rceil} \prod_{i=1}^{z} p_i^{3\lceil \frac{a_i-1}{2} \rceil}$$

By the chinese remainder theorem, this congruence can be studied by parts. First I consider the congruence:

$$n^3 2^{\alpha+2} 3^{\beta} \prod_{i=1}^{z} p_i^{a_i} \equiv 0 \mod 2^{3\lfloor \frac{\alpha}{2} \rfloor}$$

If $\alpha + 2 \geq 3\lfloor \frac{\alpha}{2} \rfloor$ then this congruence is trivially true, and no properties need to be given to n. If the previous inequality does not hold then it must be that

$$n^3 3^{\beta} \prod_{i=1}^{z} p_i^{a_i} \equiv 0 \mod 2^{3\lfloor \frac{\alpha}{2} \rfloor - \alpha - 2}$$

And by Euclid's lemma this can be simplified to

$$n^3 \equiv 0 \mod 2^{3\lfloor \frac{\alpha}{2} \rfloor - \alpha - 2}$$

Which is true whenever

$$n \equiv 0 \mod 2^{\left\lceil \frac{3\lfloor \frac{\alpha}{2} \rfloor - \alpha - 2}{3} \right\rceil}$$

This previous congruence makes perfect sense for all values of α except for $\alpha = 1$ when the congruence states that $n \equiv 0 \mod 2^{-1}$. Therefore, special consideration needs to be

made for the case $\alpha = 1$. Consider a function $f(x)$ that is equal to 1 whenever $x \neq 1$ and is equal to 0 when $x = 1$. Then a way to fix the congruence would be by stating

$$n \equiv 0 \mod 2^{f(\alpha)\left\lceil \frac{3\lfloor \frac{\alpha}{2} \rfloor - \alpha - 2}{3} \right\rceil}$$

Next it should be that

$$n^3 2^{\alpha+2} 3^{\beta} \prod_{i=1}^{z} p_i^{a_i} \equiv 0 \mod 3^{3\lceil \frac{\beta}{2} \rceil}$$

Assuming that $\beta < 3\lceil \frac{\beta}{2} \rceil$ then this simplies to

$$n^3 \equiv 0 \mod 3^{3\lceil \frac{\beta}{2} \rceil - \beta}$$

Which is true whenever

$$n \equiv 0 \mod 3^{\left\lceil \frac{3\lceil \frac{\beta}{2} \rceil - \beta}{3} \right\rceil}$$

The previous inequality is true whenever $\beta > 0$ but notice that when $\beta = 0$ the previous congruence reduces to $n \equiv 0 \mod 1$ which is always true and thus no special considerations need to be made for β.

Finally, it must be that

$$n^3 2^{\alpha+2} 3^{\beta} \prod_{i=1}^{z} p_i^{a_i} \equiv 0 \mod p_i^{3\lceil \frac{a_i - 1}{2} \rceil}$$

Assuming that $a_i \leq 3\lceil \frac{a_i - 1}{2} \rceil$ then this can be simplified into

$$n^3 \equiv 0 \mod p_i^{3\lceil \frac{a_i - 1}{2} \rceil - a_i}$$

which implies

$$n \equiv 0 \mod p_i^{\left\lceil \frac{3\lceil \frac{a_i - 1}{2} \rceil - a_i}{3} \right\rceil}$$

Which is valid for any a_i. By the chinese remainder theorem, the three necessary congruences merge into

$$n \equiv 0 \mod 2^{f(\alpha)\left\lceil \frac{3\lfloor \frac{\alpha}{2} \rfloor - \alpha - 2}{3} \right\rceil} 3^{\left\lceil \frac{3\lceil \frac{\beta}{2} \rceil - \beta}{3} \right\rceil} \prod_{i=1}^{z} p_i^{\left\lceil \frac{3\lceil \frac{a_i - 1}{2} \rceil - a_i}{3} \right\rceil}$$

And therefore

$$n = q 2^{f(\alpha)\left\lceil \frac{3\lfloor \frac{\alpha}{2} \rfloor - \alpha - 2}{3} \right\rceil} 3^{\left\lceil \frac{3\lceil \frac{\beta}{2} \rceil - \beta}{3} \right\rceil} \prod_{i=1}^{z} p_i^{\left\lceil \frac{3\lceil \frac{a_i - 1}{2} \rceil - a_i}{3} \right\rceil}, q \in \mathbb{Z}$$

so

$$\frac{n}{2^{\lfloor\frac{\alpha}{2}\rfloor}3^{\lceil\frac{\beta}{2}\rceil}\prod_{i=1}^{z}p_i^{\lceil\frac{a_i-1}{2}\rceil}}=\frac{q2^{f(\alpha)\left\lceil\frac{3\lfloor\frac{\alpha}{2}\rfloor-\alpha-2}{3}\right\rceil}3^{\left\lceil\frac{3\lceil\frac{\beta}{2}\rceil-\beta}{3}\right\rceil}\prod_{i=1}^{z}p_i^{\left\lceil\frac{3\lceil\frac{a_i-1}{2}\rceil-a_i}{3}\right\rceil}}{2^{\lfloor\frac{\alpha}{2}\rfloor}3^{\lceil\frac{\beta}{2}\rceil}\prod_{i=1}^{z}p_i^{\lceil\frac{a_i-1}{2}\rceil}}$$

$$=\frac{q}{2^{\lfloor\frac{\alpha}{2}\rfloor-f(\alpha)\left\lceil\frac{3\lfloor\frac{\alpha}{2}\rfloor-\alpha-2}{3}\right\rceil}3^{\lceil\frac{\beta}{2}\rceil-\left\lceil\frac{3\lceil\frac{\beta}{2}\rceil-\beta}{3}\right\rceil}\prod_{i=1}^{z}p_i^{\lceil\frac{a_i-1}{2}\rceil-\left\lceil\frac{3\lceil\frac{a_i-1}{2}\rceil-a_i}{3}\right\rceil}}}$$

The previous reasoning proves the following theorem:

Theorem 4. (a,b) is a fourth degree integer point if and only if it is of the form

$$\left(\frac{\pm q}{A},\frac{\pm q}{A}\pm 2^{\alpha}3^{\beta}\prod_{i=1}^{z}p_i^{a_i}\right)$$

With $z,\alpha,\beta,a_i\in\mathbb{N}_0, q\in\mathbb{Z}$, p_i arbitrary primes bigger than 3 and

$$A=2^{\lfloor\frac{\alpha}{2}\rfloor-f(\alpha)\left\lceil\frac{3\lfloor\frac{\alpha}{2}\rfloor-\alpha-2}{3}\right\rceil}3^{\lceil\frac{\beta}{2}\rceil-\left\lceil\frac{3\lceil\frac{\beta}{2}\rceil-\beta}{3}\right\rceil}\prod_{i=1}^{z}p_i^{\lceil\frac{a_i-1}{2}\rceil-\left\lceil\frac{3\lceil\frac{a_i-1}{2}\rceil-a_i}{3}\right\rceil}$$

With

$$f(x)=\begin{cases}0 & \text{if } x=1\\ 1 & \text{otherwise}\end{cases}$$

With this theorem it is clear that for the lines $y=x+c$, with c ranging from -6 to 6, the only ones with non-trivial integer points will be for $c=\pm 4$. which contains points like (-0.5,-4.5) with $(-0.5)^4-(-4.5)^4=-410$.

6. Closing remarks

It is possible to use theorem 4 to find a characterization of fifth degree integer points by the same method of finding a congruence that must be satisfied and then finding what properties must q have to satisfy the congruence. Similarly, it is probably possible to do this forever, but it will just yield uglier and uglier expressions.

6.1. An interesting sequence

Consider the line $y=x+c$, for positive c. Consider the highest degree a non-trivial integer point that is contained in the line can have. Call this number s_c. For example, $s_1=2$ as there are no non-trivial integer points of degree 3 in the line $y=x+1$ (see theorem 3) but there are non-trivial integer points of degree 2, for example (0.5,0.5 + 1).

This sequence, written down starting from c=1 and up to c=25 looks like:
$(2,2,3,4,2,3,2,4,3,2,2,4,2,2,3,6,2,3,2,3,3,2,2,4,3,...)$

Applying the theorems proven in this paper many properties of this sequence can be proven. For example that it will never be smaller than 2, and that it is unbounded. And that if c is the squarefree product of any primes not equal to 3, then $s_c=2$.

References

[1] Problem 201 - http://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf
[2] Graphs done using http://www.desmos.com