Number Theory: Heavy Machinery

Evan Chen

December 23, 2019
DNW-HEAVYNUMTH, OTIS*

§1 Lecture notes

§1.1 Quadratic and cubic equations

Unlike exponentials, these equations tend to have *lots of solutions*. Here are some classes these things.

First, a **Pell equation** is something that looks like $x^2 - ny^2 = 1$ where n is squarefree.

These are related to algebraic number theory.

Definition 1.1. Given $\alpha \in \mathbb{Q}(\sqrt{n})$ we define

$$\|\alpha\| = \left\|a + b\sqrt{n}\right\| = a^2 - nb^2.$$

Theorem 1.2

This norm is multiplicative.

Proof. In fact, it is the determinant of the linear map

$$\times\alpha \colon \mathbb{Q}(\sqrt{n}) \to \mathbb{Q}(\sqrt{n})$$

viewed as a two-dimensional $\mathbb{Q}$-vector space.

Alternatively, you can just check directly

$$\left(a^2 - nb^2\right)\left(c^2 - nd^2\right) = (ac + nbd)^2 - n\left(ad + bc\right)^2. \qquad \square$$

Remark 1.3. In fact, if you like algebraic number theory: let id and σ be the two embeddings $\mathbb{Q}(\sqrt{n}) \hookrightarrow \mathbb{C}$. Then $\|\alpha\| = \mathrm{id}(\alpha)\sigma(\alpha)$. One can use this to define the norm for anything that's not $\mathbb{Q}(\sqrt{n})$. (One may also use the determinant definition.)

Let us see an example of how this can be used. Suppose we want to generate solutions to $x^2 - 2y^2 = 1$. We start by observing that $(3, 2)$ is a solution; this is the same as saying $3 + 2\sqrt{2}$ has norm 1. Then we can consider

$$\left(3 + 2\sqrt{2}\right)^2 = 17 + 12\sqrt{2}$$

which will also have norm $1^2 = 1$; and indeed $(17, 12)$ is a solution too. Going further,

$$\left(3 + 2\sqrt{2}\right)^3 = 99 + 70\sqrt{2}$$

reveals the solution $(99, 70)$.

It is a theorem (which we will not prove) that in fact $(3 + 2\sqrt{2})^n$ will generate all solutions. More generally:

Theorem 1.4 (Pell equations generated by a unit)

Let n be a positive squarefree integer and consider the Pell equation $x^2 - ny^2 = 1$.

Then there exists a pair (x_1, y_1) of positive integers satisfying $x_1^2 - ny_1^2 = 1$ and such that all other solutions (x, y) are obtained by writing

$$x + y\sqrt{n} = \left(x_1 + y_1\sqrt{n}\right)^k$$

for some positive integer k.

Variants are $x^2 - ny^2 = -1$ and so on. For this, we just need a single α with $\|\alpha\| = \text{RHS}$, then we can multiply on by a unit.

Another quadratic family is the dreaded **Vieta jumping**: In its most basic form, if you have a symmetric two-variable equation of the form $P(x, y) = 0$ Vieta jumping lets you generate a **2-regular multigraph** on the set of $\mathbb{Z}$ solutions: if (x_0, y_0) is a solution there should be another solution of the form $(x_0, -)$ and another solution of the form $(-, y_0)$. One then often applies some monovariant or otherwise to try to show the resulting graph is a path/acyclic/etc. in order to either classify all solutions or at least show that infinitely many exist.

Example 1.5 (IMO 1988/6)

Let a and b be positive integers. Prove that if

$$\frac{a^2 + b^2}{ab + 1}$$

is also an integer, then it is a perfect square.

Walkthrough. Let $k = \frac{a^2+b^2}{ab+1}$ be fixed. We will show k is a perfect square.

I want to start with an observation that we'll need later on. The reason I put it here this early is to make sure you realize that it's trivial (and does not require Vieta jumping), before we get lost in the meat of the solution.

(a) Prove that any solution to this equation must satisfy $\min(a, b) \geq 0$.

The idea behind Vieta jumping is to write this as a quadratic equation

$$a^2 - kb \cdot a + b^2 - k = 0$$

in a; thus for a fixed value of b, we can then "flip" the quadratic in a to get the other value. One might write this as

$$(a,b) \mapsto (k \cdot b - a, b) = \left(\frac{b^2-k}{a}, b \right).$$

Let's do some concrete practice so you can see what I mean.

(b) Let $k = 4$ and observe that $(a,b) = (30,8)$. Write the quadratic and see how you could realize that $(a,b) = (2,8)$ was also a solution.

(c) Flip in the other direction: find the other value of b which works with $a = 30$.

(d) Now let's take $(a,b) = (2,8)$ and flip again, holding $a = 2$ fixed and changing the value of b. What do we get for the other value of b this time?

Thus we see in this problem that every (a,b) automatically has two natural neighbors, one obtained by flipping a and flipping b.

Our goal is to now do this flipping operation in such a way that the pair gets smaller, and see what happens if we keep doing this until we get stuck. (Local, anyone?)

(e) Show that if (a,b) is a solution with $a > b > 0$, then by Vieta jumping we can produce a solution (a',b) with $a' < b$ (but not necessarily $a' > 0$).

(f) Reconcile (a) and (e) to show that we eventually may arrive at a pair in which one component is zero.

(g) Conclude that k is a perfect square.

Example 1.6 (HMMT 2017 A8)

Suppose a and b are positive integers such that

$$c = \frac{(a+b)(a+b+1)}{ab}$$

is an integer. Find all possible values of c.

Walkthrough. I'll let you try this one mostly on your own. As a hint, it's easier I think to write this as

$$k \stackrel{\text{def}}{=} c - 2 = \frac{a^2+b^2+a+b}{ab}$$

since there are fewer terms that way.

(a) Show that the only minimal solutions are $(1,1)$ and $(2,2)$ by Vieta jumping.

(b) Write explicitly the first few solutions in the family for each of $c = 5$, $c = 6$.

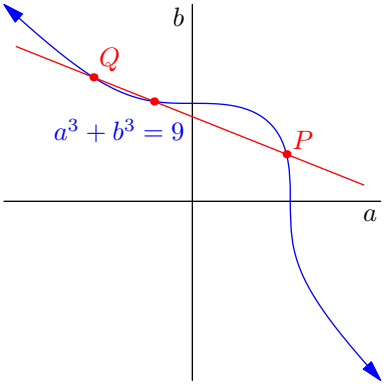
In degree 3 we have **elliptic curves**.

Example 1.7

Give a nontrivial example of two rational numbers (a,b) such that $a^3 + b^3 = 9$.

Walkthrough. The idea behind the group law of an elliptic curve shows here.

(a) Consider two rational points P and Q on the curve (here by "rational" we mean a point (a, b) with two rational coordinates). Assume that line PQ intersects the curve again at a point R. Show that R also has rational coordinates. (Possible hint: Vieta formulas.)



(b) Try to apply the procedure in (a) to the two "obvious" rational points $(1, 2)$ and $(2, 1)$. What goes wrong?

(c) Fix this by repeating the procedure with $P = Q = (2, 1)$ instead. (What does line PQ mean in that case?) You should find that this procedure spits out the point

$$(a, b) = \left(\frac{20}{7}, -\frac{17}{7}\right).$$

Example 1.8 (USAMO 2015/1)
Solve in integers the equation

$$x^2 + xy + y^2 = \left(\frac{x+y}{3} + 1\right)^3.$$

Walkthrough. We first begin by exploiting the symmetry to pick better variables:

(a) Show that the equation rewrites as

$$3a^2 + b^2 = 4\left(\frac{a}{3} + 1\right)^3$$

where $a = x + y$ and $b = x - y$.

(b) Prove that $3 \mid a$, so let $a = 3c$. This gives us a curve in (b, c).

At this point the equation becomes

$$b^2 = 4c^3 - 15c^2 + 12c + 4.$$

This is in the shape of an elliptic curve, and it's hopeless to find solutions in general to those using high-school methods except in really stupid situations (e.g. $y^2 = 2x^3$ or $2y^2 = 2x^3 + 1$ or something). This means that the coefficients on the right-hand side have to be really special in some way for the problem to be doable.

(c) Factor the right-hand side.

(d) Show that $4c + 1$ is a square, and use this to write down a pair (x, y) of solutions.

(e) Verify the first few solutions you get are $(-1, 1)$, $(3, 3)$, $(19, -1)$, $(53, -17)$, ...

§1.2 Some more theorems

- Mihăilescu theorem / Catalan conjecture: The only consecutive perfect powers are 8 and 9.
- Bertrand postulate: For all $n \geq 1$, there is a prime between n and $2n$.
- Dirichlet: If $\gcd(a, m) = 1$, then there exist infinitely many primes $p \equiv a \pmod{m}$.
- Kobayashi: Let M be an infinite set and $0 \neq a \in \mathbb{Z}$. If only finitely many primes divide some element of M, then infinitely many primes divide some element of $M + a$.

Example 1.9 (Iran TST 2009/2)
Let a be a positive integer. Prove that there are infinitely many primes dividing some number of the form $2^{2^n} + a$.

§1.3 Jacobi symbol and quadratic reciprocity

Quadratic residues occupy "half" the nonzero residues modulo a prime.

The quadratic reciprocity formula specifies how to check if $a \pmod{p}$ is a quadratic residue.

Definition 1.10. For a prime p and integer a, set

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \not\equiv 0 \text{ is a quadratic residue} \\ -1 & a \not\equiv 0 \text{ is not a quadratic residue.} \end{cases}$$

This is called a **Legendre symbol**.

Proposition 1.11 (Legendre's definition)
For odd primes p, $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$.

It follows that the Legendre symbol $\left(\frac{\bullet}{p}\right)$ is multiplicative in the top.

The Jacobi symbol is cooler than the Legendre symbol.

Definition 1.12. The **Jacobi symbol** $\left(\frac{a}{n}\right)$ is defined by extending the Legendre symbol completely multiplicatively in the bottom; that is,

$$\left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right).$$

Hence the Jacobi symbol is completely multiplicative in both parts. It also satisfies:

- $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ when $a \equiv b \pmod{n}$.
- $\left(\frac{a}{n}\right) = 0$ if and only if $\gcd(a, n) > 1$ (and is otherwise ± 1).
- $\left(\frac{a}{2}\right) \in \{0, 1\}$ for all a.

Remark 1.13. Warning: $\left(\frac{a}{n}\right)$ doesn't detect quadratic residues modulo n anymore if n is not prime. For example, 2 isn't a quadratic residue modulo *either* 3 or 5, so it is definitely not a quadratic residue modulo 15 either. But $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)^2 = +1$.

Most importantly, quadratic reciprocity is usually stated for primes, but the statement for Jacobi symbols is cooler.

Theorem 1.14 (Quadratic Reciprocity, with Jacobi symbols)

Let m and n be relatively prime positive odd integers. Then

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(n-1)} \qquad \left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)} \qquad \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)}.$$

This means you can compute $\left(\frac{481}{2017}\right)$ or $\left(\frac{551}{2011}\right)$, for example, without having to factor the numerator. The former one is:

$$\left(\frac{481}{2017}\right) \overset{\text{QR}}{=} \left(\frac{2017}{481}\right) = \left(\frac{93}{481}\right) \overset{\text{QR}}{=} \left(\frac{481}{93}\right) = \left(\frac{16}{93}\right) = +1.$$

Thus using the Jacobi symbol instead of the Legendre one makes quadratic reciprocity more powerful (and is indeed one main reason for introducing it).

§1.4 Zsigmondy practice

Theorem 1.15 (Zsigmondy, first form)

Let $a > b > 0$ be relatively prime positive integers. Then for every $n > 1$ there's a prime dividing $a^n - b^n$ and not dividing $a^k - b^k$ for $k < n$, with two exceptions:

- $(a, b, n) = (2, 1, 6)$.
- $n = 2$, and $a + b$ is a power of 2.

The condition $n > 1$ is there to deal with the dumb situation where $a - b = 1$. There's a second form of the theorem which follows from the first one.

Theorem 1.16 (Zsigmondy, second form)

Similarly, there's a prime dividing $a^n + b^n$ and not $a^k + b^k$ for $k < n$ with one exception:

- $(a, b, n) = (2, 1, 3)$.

Example 1.17 (Italy TST 2003)

Solve $2^a + p^b = 19^a$ where p is a prime number, and a, b are positive integers.

Example 1.18 (Shortlist 2002 N3)

Let $p_1, \ldots, p_n$ be distinct primes greater than 3. Prove that $2^{p_1 p_2 \cdots p_n} + 1$ has at least 4^n divisors.

Example 1.19 (Shortlist 2000 N4)
Find all triples (a, m, n) of positive integers for which $a^m + 1 \mid (a+1)^n$.

Example 1.20 (China TST Quiz 2005; also Shortlist 1997; also Blue MOP 2012)
Let b, m, n be positive integers such that $b > 1$ and $m \neq n$. Prove that if $b^m - 1$ and $b^n - 1$ have the same prime divisors then $b + 1$ is a power of 2.

§1.5 Actual Problems

Example 1.21 (Taiwan TST)
Let m and n be relatively prime positive integers. Prove that $\varphi(5^m - 1) \neq 5^n - 1$.

Walkthrough. This is one of my favorite QR problems. Assume for contradiction (m, n) works.

(a) Assume m is even. Deduce that n is odd, and by considering ν_2's, derive a contradiction. Hence we may assume m is odd.

(b) Show that $5^m - 1$ is squarefree. Hence we may write

$$5^m - 1 = 4p_1p_2 \cdots p_k \tag{1}$$
$$5^n - 1 = 2(p_1 - 1)(p_2 - 1) \cdots (p_k - 1) \tag{2}$$

where the p_i are distinct odd primes.

(c) Using QR, show that any odd prime dividing $5^m - 1$ for m odd must be $\pm 1 \pmod 5$. (Apparently, people don't know you can do this anymore!)

(d) Deduce that in the context of this problem, we have $p_i \equiv 4 \pmod 5$ for all i.

(e) Find a contradiction on the value of k by taking the equations modulo 5 now.

Also, a problem with a story (Eric Lander):

Example 1.22 (Putnam 1976 B6)
Prove that if n is an integer such that the divisors of n have sum exactly $2n + 1$, then n is the square of an odd integer.

Walkthrough. The first part is pretty easy:

(a) Show that n is a square.

Thus the main effort is to show n is odd. Let $n = 2^e k^2$ where $e \geq 0$ is even.

(b) Show that $2^{e+1} - 1 \mid 2n + 1$.

(c) Evaluate $k^2 \pmod{2^{e+1} - 1}$.

(d) Deduce a contradiction for $e > 0$.

See the remark at the end of the solution for a story about the problem.

§2 Practice problems

Instructions: Solve [40♣]. If you have time, solve [60♣]. Problems with red weights are mandatory.

> I have all these great genes, but they're recessive.
>
> Calvin in *Calvin and Hobbes*

[2♣] **Problem 1.** Solve the equation $a^2 + b^2 + c^2 = (ab)^2$ over the integers.

[3♣] **Problem 2** (PUMaC 2016)**.** Find the sum of the four smallest primes dividing $2016^{239} - 1$.

[2♣] **Problem 3** (Schinzel)**.** Find all integers $n \geq 1$ such that n divides $2^{n-1} + 1$.

[3♣] **Problem 4.** Prove that $2^n + 1$ has no prime factors of the form $p = 8k + 7$.

[3♣] **Problem 5** (RMM 2013/1)**.** For a positive integer a, define a sequence of integers $x_1, x_2, \ldots$ by letting $x_1 = a$ and $x_{n+1} = 2x_n + 1$ for $n \geq 1$. Let $y_n = 2^{x_n} - 1$. Determine the largest possible k such that, for some positive integer a, the numbers $y_1, \ldots, y_k$ are all prime.

[3♣] **Problem 6** (PUMaC 2013 N8)**.** Find the number of primes p between 100 and 200 for which $x^{11} + y^{16} \equiv 2013 \pmod{p}$ has a solution in integers x and y.

[3♣] **Problem 7** (Romania TST 2008/3/3)**.** Let a and b be positive integers such that $2^a - 1$ divides $3^b - 1$. Prove that either $a = 1$ or b is even.

[3♣] **Problem 8** (PRIMES 2019 M5)**.** Exhibit a function $s \colon \mathbb{Z}_{>0} \to \mathbb{Z}$ with the following property: if a and b are positive integers such that $p = a^2 + b^2$ is an odd prime, then

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

[5♣] **Problem 9** (TSTST 2013/8)**.** Define a function $f \colon \mathbb{N} \to \mathbb{N}$ by $f(1) = 1$, $f(n+1) = f(n) + 2^{f(n)}$ for every positive integer n. Prove that $f(1)$, $f(2)$, $\ldots$, $f(3^{2013})$ leave distinct remainders when divided by 3^{2013}.

[2♣] **Problem 10** (MOP 2007)**.** Prove that there are infinitely many pairs of positive integers (m, n) such that

$$\frac{m+1}{n} + \frac{n+1}{m}$$

is an integer.

[3♣] **Problem 11** (Shortlist 2017 N6)**.** Find the smallest positive integer n such that the following holds: there exist infinitely many n-tuples $(a_1, \ldots, a_n)$ of positive rational numbers for which

$$a_1 + \cdots + a_n \qquad \text{and} \qquad \frac{1}{a_1} + \cdots + \frac{1}{a_n}$$

are both integers.

[3♣] **Problem 12** (APMO 2014/3)**.** Find all positive integers n such that for any integer k there exists an integer a for which $a^3 + a - k$ is divisible by n.

[3♣] **Problem 13** (EGMO 2016/6)**.** Let S be the set of all positive integers n such that n^4 has a divisor in the range $n^2 + 1$, $n^2 + 2$, $\ldots$, $n^2 + 2n$. Prove that there are infinitely many elements of S of each of the forms $7m$, $7m + 1$, $7m + 2$, $7m + 5$, $7m + 6$ and no elements of S of the form $7m + 3$ and $7m + 4$, where m is an integer.

[5♣] **Problem 14** (January TST 2013/1)**.** Two incongruent triangles ABC and XYZ are called a pair of *pals* if they satisfy the following conditions:

1. the two triangles have the same area;
2. let M and W be the respective midpoints of sides BC and YZ. The two sets of lengths $\{AB, AM, AC\}$ and $\{XY, XW, XZ\}$ are identical 3-element sets of pairwise relatively prime integers.

Determine if there are infinitely many pairs of triangles that are pals of each other.

[5♣] **Problem 15** (IMO 2003/2)**.** Determine all pairs of positive integers (a, b) such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

[5♣] **Problem 16** (ELMO 2011/5)**.** Let $p > 13$ be a prime of the form $2q + 1$ where q is prime. Find the number of ordered pairs of integers (m, n) such that $0 \le m < n < p - 1$ and

$$3^m + (-12)^m \equiv 3^n + (-12)^n \pmod{p}.$$

[3♣] **Problem 17** (Romania TST 2004/2/2)**.** If a and b are two positive integers such that $ab \neq 1$, we define

$$f(a, b) = \frac{a^2 + ab + b^2}{ab - 1}.$$

Find all integer values that $f(a, b)$ can take.

[9♣] **Problem 18** (USA TST 2014/2)**.** Let a_1, a_2, a_3, ... be a sequence of integers, with the property that every consecutive group of a_i's averages to a perfect square. More precisely, for all positive integers n and k, the quantity

$$\frac{a_n + a_{n+1} + \cdots + a_{n+k-1}}{k}$$

is always the square of an integer. Prove that the sequence must be constant (all a_i are equal to the same perfect square).

[9♣] **Problem 19** (Iran TST 2013)**.** Do there exist positive integers a, b and c such that $a^2 + b^2 + c^2$ is divisible by $2013(ab + bc + ca)$?

[1♣] **Mini Survey.** At the end of your submission, answer the following questions.

(a) About how many hours did the problem set take?

(b) Name any problems that stood out (e.g. especially nice, instructive, boring, or unusually easy/hard for its placement).

Any other thoughts are welcome too. Examples: suggestions for new problems to add, things I could explain better in the notes, overall difficulty or usefulness of the unit.

§3 Solutions to the walkthroughs

§3.1 Solution 1.5, IMO 1988/6

Let $k = \frac{a^2+b^2}{ab+1}$. Then rewrite it as:

$$a^2 - kb \cdot a + b^2 - k = 0.$$

Then we can do a standard Vieta jumping argument. For example, when $k = 4$ the chain goes

$$\cdots \to (112, 30) \to (30, 8) \to (8, 2) \to (2, 0).$$

So, suppose $a > b > 0$ is a solution. Then

$$(a, b) \to (k \cdot b - a, b) = \left(\frac{b^2 - k}{a}, b \right).$$

Notice that $\frac{b^2-k}{a} < a$, so flipping the larger one always decreases.

We have to rule out the possibility of negative numbers in chain. Indeed $k > 0$, so looking at $k = \frac{a^2+b^2}{ab+1}$ shows its impossible for exactly one term to be negative, so eventually one coordinate is zero.

Visibly if $b = 0$ then $k = a^2$ as desired.

§3.2 Solution 1.6, HMMT 2017 A8

We claim the answer is $c = 5$, $c = 6$. This is by Vieta jumping.

Firstly note that $\frac{(a+b)(a+b+1)}{ab} = 2 + \frac{a^2+b^2+a+b}{ab}$. Let $k = c - 2$. Consider the quadratic

$$X^2 - (bk - 1)X + b^2 + b = 0.$$

It has one root $X = a$, and the other (integer) root $\frac{b(b+1)}{a}$. In other words root flipping gives:

$$(a, b) \longleftrightarrow \left(\frac{b(b+1)}{a}, b \right).$$

Now suppose (a, b) with $a \geq b$ is a solution for some k, and moreover assume $a + b$ is minimal. We now divide into three cases:

- If $a = b$, we get $k = 2 + \frac{2}{b}$. This gives $k = 3$ for $(a, b) = (2, 2)$ and $k = 4$ for $(a, b) = (1, 1)$.
- Else if $a \geq b + 1$ then $\frac{b(b+1)}{a} < a$ and thus $(\frac{b(b+1)}{a}, b)$ is a smaller solution, contradiction.

The jumping process actually lets us characterize all pairs of solutions. One obtains the following chains for $c = 5$ and $c = 6$ (which are $k = 3$ and $k = 4$) respectively, with the arrow pointing in the direction given by the argument above.

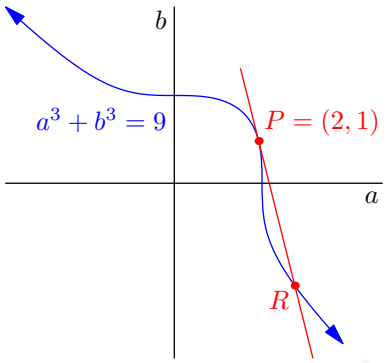
$$(2, 2) \leftrightarrow (2, 3) \leftarrow (3, 6) \leftarrow (6, 14) \leftarrow (14, 35) \leftarrow (35, 90) \leftarrow \dots$$
$$(1, 1) \leftrightarrow (1, 2) \leftarrow (2, 6) \leftarrow (6, 21) \leftarrow (21, 77) \leftarrow \dots.$$

§3.3 Solution 1.7

The point

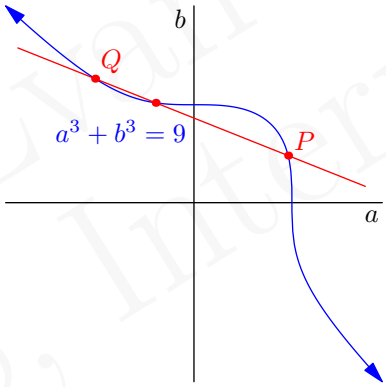
$$(a, b) = \left(\frac{20}{7}, -\frac{17}{7}\right)$$

works well. It can be found by taking the tangent to $P = (2, 1)$ and intersecting it with the curve.



Note that taking the line through $(2, 1)$ and $(1, 2)$ does not work as the resulting line $a + b = 3$ is parallel to the asymptote of the curve. In the language of the group law on elliptic curves, these two points are inverses and the identity is the infinity point!

Here is a picture of the group law in general:



§3.4 Solution 1.8, USAMO 2015/1

We do the trick of setting $a = x + y$ and $b = x - y$. This rewrites the equation as

$$\frac{1}{4}\left((a+b)^2 + (a+b)(a-b) + (a-b)^2\right) = \left(\frac{a}{3} + 1\right)^3$$

where $a, b \in \mathbb{Z}$ have the same parity. This becomes

$$3a^2 + b^2 = 4\left(\frac{a}{3} + 1\right)^3$$

which is enough to imply $3 \mid a$, so let $a = 3c$. Miraculously, this becomes

$$b^2 = (c-2)^2(4c+1).$$

So a solution must have $4c + 1 = m^2$, with m odd. This gives

$$x = \frac{1}{8}\left(3(m^2-1) \pm (m^3 - 9m)\right) \quad \text{and} \quad y = \frac{1}{8}\left(3(m^2-1) \mp (m^3 - 9m)\right).$$

For mod 8 reasons, this always generates a valid integer solution, so this is the complete curve of solutions. Actually, putting $m = 2n+1$ gives the much nicer curve

$$\boxed{x = n^3 + 3n^2 - 1 \quad \text{and} \quad y = -n^3 + 3n + 1}$$

and permutations.

For $n = 0, 1, 2, 3$ this gives the first few solutions are $(-1, 1)$, $(3, 3)$, $(19, -1)$, $(53, -17)$, (and permutations).

§3.5 Solution 1.9, Iran TST 2009/2

One word: Kobayashi.

§3.6 Solution 1.17, Italy TST 2003

Only $p = 17$, $a = b = 1$. Obviously $p = 17$, and then Zsigmondy implies no solutions exist for $a > 1$.

§3.7 Solution 1.18, Shortlist 2002 N3

In fact, by Zsigmondy theorem the number has at least 2^n distinct prime divisors, since there is a different prime divisor dividing each number of the form $2^m + 1$ where $m \mid p_1 \dots p_k$ (note $m \neq 3$). Hence at least 2^{2^n} prime divisors.

§3.8 Solution 1.19, Shortlist 2000 N4

Answer:

- $a = 1$,
- $m = 1$,
- or $(a, m) = (2, 3)$ with $n \geq 2$.

In general, Zsigmondy theorem kills the converse.

§3.9 Solution 1.20, China TST Quiz 2005; also Shortlist 1997; also Blue MOP 2012

Zsigmondy kills it except in the case $b = 2$ and $\max(m, n) = 6$ which can be checked easily by hand.

§3.10 Solution 1.21, Taiwan TST

Here is solution with Lawrence Sun. Assume for contradiction this is the case for some $m > 1$.

> **Claim —** The integer m is odd, and moreover $(5^m - 1)/4$ is squarefree.

Proof. First, we show m is odd. If not, then n is odd, but $8 \mid 5^m - 1$, and also $\nu_2(5^n - 1) = 2$, and it's impossible than $\nu_2(\varphi(8k)) = 2$ for $k > 1$.

Next, we claim that no odd prime divides $5^m - 1$ twice. Otherwise, we get that $p \mid 5^n - 1$ as well. Yet $\gcd(5^m - 1, 5^n - 1) = 5^{\gcd(m,n)} - 1 = 4$. □

Therefore, we may write

$$5^m - 1 = 4p_1p_2 \cdots p_k \tag{3}$$
$$5^n - 1 = 2(p_1 - 1)(p_2 - 1) \cdots (p_k - 1) \tag{4}$$

where the p_i are distinct odd primes. Remark that $p_i \not\equiv 1 \pmod 5$ for all i.

But now (1) gives

$$\left(5^{\frac{m+1}{2}}\right)^2 = 5^{m+1} \equiv 5 \pmod{p_i}$$

By Quadratic Reciprocity, we see that 5 is a residue modulo p_i, so each p_i is a residue modulo 5. By our remark earlier this forces $p_i \equiv -1 \pmod 5$ for all i.

Now (1) gives

$$-1 \equiv 4 \cdot (-1)^k \pmod 5$$

so that k is even. But (2) then gives

$$-1 \equiv 2 \cdot (-2)^k \pmod 5$$

which does not occur for any even k.

This is a contradiction and hence no solutions exist.

> **Remark.** A difficult proof that $\gcd(m, n) = 1$ can be dropped is listed at http://www.mathnet.or.kr/mathnet/thesis_file/BKMS-52-2-513-524.pdf.
>
> I've been told this was on Taiwan TST 2000 in https://aops.com/community/q1h1606654p10064881 but can't confirm this.

§3.11 Solution 1.22, Putnam 1976 B6

For any prime p with $\nu_p(n) = e$, we know that is divisible by $1 + p + p^2 + \cdots + p^e$. For p odd this immediately implies e is even for parity reasons. The tricky part is to show that 2 cannot divide n.

Let $n = 2^e k^2$, and assume for contradiction $e > 0$. Then $\sigma(n)$ is divisible by $1 + 2 + \cdots + 2^e = 2^{e+1} - 1$. Now take $q \mid 2^{e+1} - 1$ with $q \equiv 3 \pmod 4$ prime. Then we have

$$2 \cdot 2^e k^2 + 1 \equiv 0 \pmod q \implies k^2 \equiv -1 \pmod q$$

which is a contradiction.

> **Remark.** Here is a legend about this problem I heard at the IMO (whose accuracy I won't attest to).
>
> An integer n is called *quasiperfect* if it satisfies this condition. In 1974, Eric Lander won the Westinghouse talent search (which these days is now known as Intel or Regeneron) with a high-school research paper which included this result. For context, Eric Lander was on the very first American IMO team, and is now a professor of biology at MIT.
>
> Anyways, one of the reviewers of Eric's high-school paper thought the result was nice, and noted it down. It thus appeared on the 1976 Putnam as problem B6 — on which Eric Lander was a contestant.