A lively activity: To do mathematics

Diophantine equations

15 May 1982

Summary: *Interest in solving equations in integers or rational numbers dates back from antiquity. I tried to show some fundamental problems which are still unsolved. Euclid and Diophantus already solved the equation* $a^2 + b^2 = c^2$, *and gave a formula for all the solutions. The next hardest equation like* $y^2 = x^3 + ax + b$ *has given rise to very great problems which have been at the center of mathematics since the 19th century. No one knows how to give an effective method for finding all solutions. I described some of the structures which the solutions have, and the context in which one would like to find such a method.*

In May 1981, during a brief stay in Paris, Serge Lang gave us a conference on prime numbers, showing some of the motivation which leads a mathematician to "do mathematics".

The welcome given him by the audience, the curiosity and enthusiasm of certain students who had attended his talk led him to renew the experience this year, and we are all grateful to him for doing so.

The following text was written in the same spirit as the one last year; that is, to preserve as far as possible Serge Lang's lively tone and style. The text reflects the exchange, with one deletion and a few additions. The deletion concerned an exchange on problems of high school teaching. It was either too general, or on the contrary too personal, and the questions did not seem to shed any light on this topic, so we decided to delete it. On the other hand, since Serge Lang prefers to *do* things rather than to talk about "what could be done?", the reader who would like to know more precisely how he conceives a mathematics book at this level can consult his *Basic Mathematics*,* or the book *Geometry*, written together with Gene Murrow.†

The additions deal with certain mathematical points which could not be discussed for lack of time. These points illustrate, in a certain way, the patience and kindness with which Serge Lang, in the following weeks, accepted to answer all my questions, including those which today appear rather naive. I take this occasion to express my thanks.

The last pages of the conference, concerning some conjectures about the size of solutions, were added six months later, and showed at the time, if it was still necessary, that the conference dealt with live mathematics, mathematics in the process of being done. Since then, one could not have found a better proof of the vitality and relevance of mathematical research: Mordell's conjecture (p. 55) which was about sixty years old, was proved by Gerd Faltings in Germany. This first rate result was obtained in part by using the vast resources of algebraic geometry, developed mainly during these last thirty years; and in part by relying on the work of the Soviet school of mathematics. This is a relatively frequent situation in mathematics, when a great personal contribution takes place in the context of the work developed by an active mathematical community.

J.B.

---

* Addison-Wesley, 1971 (out of print).

† Springer-Verlag, 1983.

The conference

SERGE LANG. The goal of this talk is again to do mathematics together. For those who were not here last year, I'll start with a few minutes of more general comments. Last time, I asked: "What does mathematics mean to you?" And some people answered: "The manipulations of numbers, the manipulation of structures." And if I had asked what music means to you, would you have answered: "The manipulation of notes?" So I ask again: What does mathematics mean to you?

GENTLEMAN. It's to work with numbers.

SERGE LANG. No, no! It's not to work with numbers.

A HIGH SCHOOL STUDENT. It's to solve a problem.

SERGE LANG. There, you are getting closer. Solve a problem. That's what I had tried to show you last time. That it was not just to manipulate something. It strikes much more deeply into our psychology, and unfortunately there is nothing, or almost nothing, except for certain exceptionally gifted teachers, there is nothing in our elementary schools or high schools which allows people to realize what mathematics is about, or what it means to do mathematics. Just before the conference, I was looking at a tenth grade textbook in Mr. Brette's office (he organized this conference), and it's to vomit. [*Whisperings in the audience.*] It's to vomit, from all points of view: the general incoherence, which goes from beginning to end; the little problems which don't mean anything; the aridity of the exposition . . . It's disgusting. [*Agitation in the audience, some laughter.*]

QUESTION. Can you tell us the name of the book?

SERGE LANG. Oh! I could have brought it down here, I wouldn't mind! You know, I'm not afraid to say what I think. But I left it upstairs. Anyhow, these things are practically all alike. [*Laughter.*] You know, those things are homogeneous. So what I am trying to do now, is to show you something else; to show you why mathematicians do mathematics, and spend their life doing it. That's what I am trying to show you.

Last time, we also talked about the role of pure and applied mathematics, of the relations between them, very briefly. And I read a quote from von Neumann, when he complained about what he called "baroque" mathematics. He said:

> As a mathematical discipline travels far from its empirical sources, or still more, if it is a second and third generation only indirectly inspired by ideas coming from "reality", it is beset with very grave dangers. It becomes more and more purely aestheticizing, more and more *l'art pour l'art* . . . at a great distance from its empirical source . . . a mathematical subject is in danger of degeneration.

So he was complaining. But there is another quote from von Neumann which one should read to those people who pester us with the first, and don't know or don't mention the second. I am going to read it to you.

> But still a large part of mathematics which became useful developed with absolutely no desire to be useful, and in situations where nobody could possibly know in what area it would become useful; and there were no general indications that it ever would be so. By and large it is uniformly true in mathematics that there is a time lapse between a mathematical discovery and the moment when it is useful; and that this lapse of time can be anything from thirty to a hundred years, in some cases even more; and that the whole system seems to function without any direction, without any reference to usefulness . . . This is true for all of science. Successes were largely due to forgetting completely about what one ultimately wanted, or whether one wanted anything ultimately; in refusing to investigate things which profit, and in relying solely on guidance by criteria of intellectual elegance; it was by following this rule that one actually got ahead in the long run, much better than any strictly utilitarian course would have permitted.
>
> I think that this phenomenon could be studied very well in mathematics; and I think everyone in science is in a very good position to satisfy himself as to the validity of these views. And I think it extremely instructive to watch the role of science in everyday life, and to note how in this area the principle of *Laissez faire* has led to strange and wonderful results. [vN]

There is nothing like saying contradictory things to be always right. [*Laughter.*]

OK, that's enough general comments, let's do mathematics.

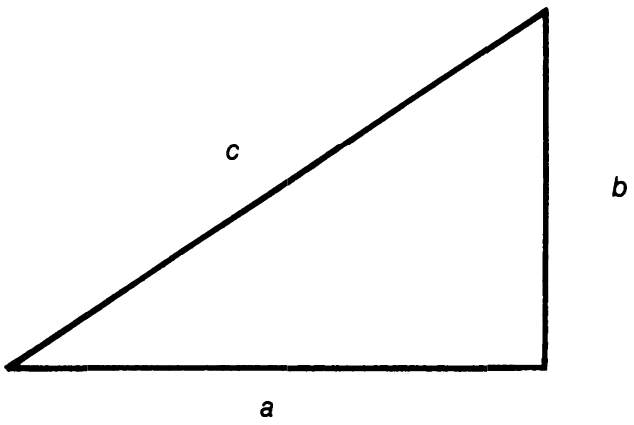
Of course, as I said last year, I am forced to choose topics which are in principle understandable by everybody. This means that most of mathematics is completely excluded. And it is also true that there will be numbers in the subject I have chosen for today. But it is not so much the presence of numbers that counts, as the way we are going to deal with them and think about them.

We can start without numbers, just as Pythagoras would have done, by taking a right triangle, with sides a, b, c. I suppose that everybody remembers Pythagoras' theorem, which says what? [*Serge Lang points to a young man in the audience. Laughter.*]

YOUNG MAN. The sum of the squares . . .

SERGE LANG. Yes, so what is the first square? It's a. . .

YOUNG MAN. a squared plus b squared equals c squared.



SERGE LANG. That's right, it's the equation

$$a^2 + b^2 = c^2.$$

Now, do you know any solutions of this equation in integers? Everybody knows what an integer is? 1, 2, 3, 4, 5, 6 and so on. So are there solutions with integers?

THE AUDIENCE. 3, 4, 5.

SERGE LANG. No, wait! I am asking the guy here. [*Laughter.*] Let me choose. [*Laughter again.*] And especially, the rules of the game: there are probably, and even certainly, a number of mathematicians in the audience. I ask them not to intervene, it's not for them that I am giving this talk and if they intervene, it's cheating! All right, let's go back to the young man over here. Give me a solution.

YOUNG MAN. 3 squared plus 4 squared equals 5 squared.

SERGE LANG. Yes. Now is there another one? Well, let's take a vote, we do this very democratically. You, sir, you say no. The gentleman over there thinks the answer is yes. Who says no? Raise your hand. Who says yes? There is quite a lot of yes. Those who say yes, give me another solution. Sir?

THE GENTLEMAN. [*No answer.*]

SERGE LANG. You said yes.

GENTLEMAN. I know that there are many other solutions, but it is a little difficult to say which ones.

SERGE LANG. All right, is there any one who knows another one?

THE AUDIENCE. 5, 12, 13.

SERGE LANG. It works, $25 + 144 = 169$.

A HIGH SCHOOL STUDENT. If you have one, (a, b, c), and if d is any number, then (da, db, dc) will also work.

SERGE LANG. Right, if (a, b, c) is a solution and if you multiply by an integer d, then you get another solution:

$$(da)^2 + (db)^2 = (dc)^2.$$

Therefore, the reasonable question is: are there other solutions besides the two we already know, and their multiples?

Who says yes? Who says no? Who keeps a prudent silence? [*Laughter.*] In any case, we are facing a problem which the Greeks already knew. Well, what we are going to do in the next five or ten minutes, is to find all the solutions, and I will prove it. How do I prove it? I write them all down. But since I can't write them down one after another, because there is an infinite number of them, I must have a general method. So we begin by transforming the problem a little. If I divide the equation $a^2 + b^2 = c^2$ by c^2, then I get

$$(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1.$$

I let $x = a/c$ and $y = b/c$. Then the equation $a^2 + b^2 = c^2$ becomes

$$x^2 + y^2 = 1.$$

And if a, b, c are integers, then x, y will be . . . what kind of numbers?

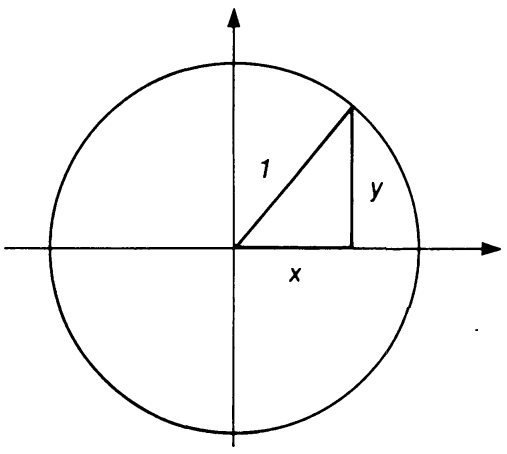
AUDIENCE. Rational numbers.

SERGE LANG. That's right. Consequently, to find one or all the solutions of $a^2 + b^2 = c^2$ in integers is equivalent to finding all the solutions of $x^2 + y^2 = 1$ in rational numbers. Because conversely, if I have a solution (x, y) in rational numbers, then I can write each number as a fraction, with a common denominator c; and then I clear denominators and I find a solution of $a^2 + b^2 = c^2$ in integers. The problem is now to find all the solutions of $x^2 + y^2 = 1$ in rational numbers.

Do you know what the equation $x^2 + y^2 = 1$ represents? What is its graph?

AUDIENCE. A circle.

SERGE LANG. Yes, we can draw it here.



It's a circle of radius 1, and with center at the origin of the axes. We have a triangle of hypotenuse 1, and sides x, y. We can state our problem by saying that we must find all the rational points on the circle, that is all the points whose coordinates x and y are rational numbers.

Before I find *all* the solutions, I am going to write down a lot of them. I let:

$$x = \frac{1 - t^2}{1 + t^2} \qquad \text{and} \qquad y = \frac{2t}{1 + t^2}.$$

I write these formulas . . .

MR. A. [*Aggressive.*] But you thought of these just like that . . .

SERGE LANG. No, I did not think of them "just like that", but someone, long ago, thought of them "just like that".

MR. A. Oh yes? Really, all of a sudden?

SERGE LANG. No, of course not, he was playing with mathematics, he was looking at a lot of things, and then he realized that it gave solutions. When he realized this, he was doing mathematics and he was being a good mathematician. But once he discovered it, then the next generations use the result, and copy it. That's all I was doing, I don't claim anything else.

MR. A. Don't you think that is precisely the difficultly for someone who does not keep up with mathematics, to find these results in order to effectively do mathematics?

SERGE LANG. Where a mathematician goes fishing for these things cannot be explained. Each mathematician gets them wherever he can. Right now, I am trying to show you a complete solution of the problem. After that, I'll show you unsolved problems. You can work on them . . . you can go fishing for them by yourself, and if the fish bites and you catch a big fish, then you get a gold medal or a chocolate medal.

ANOTHER. It comes from trigonometry, no?

SERGE LANG. It comes from wherever you want. I don't have time now to show you that in greater detail. It comes from many places simultaneously.[1]

---

[1] The question where those formulas come from arises frequently, and until today, I did not know the answer. Considering the intensity of the audience's reaction, both during the talk and afterwards, I decided to look into the history of these formulas more closely. Historically the Greeks were interested in the solutions of $a^2 + b^2 = c^2$ in integers. Euclid (three centuries BC) already knew the formulas

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2,$$

with integers m, n. Diophantus (three centuries AD) knew how to deal with fractions, and also knew that if you divide these formulas by $m^2 + n^2$ and put $t = m/n$, then you get back the formulas which I have written above. These formulas therefore certainly did not come from "trigonometry". Diophantus was interested in finding rational solutions to equations

Now let's check that our formulas do give solutions of $x^2 + y^2 = 1$. With very little algebra, you find:

$$x^2 = \frac{1 - 2t^2 + t^4}{1 + 2t^2 + t^4}, \qquad y^2 = \frac{4t^2}{1 + 2t^2 + t^4}$$

and therefore

$$x^2 + y^2 = \frac{1 + 2t^2 + t^4}{1 + 2t^2 + t^4} = 1.$$

We have therefore found an identity, which is valid for all values of t. Suppose that I substitute for t some rational number. What do I obtain for x and y?

AUDIENCE. ???

SERGE LANG. We obtain rational numbers. We obtain them from t by additions, subtractions, multiplications, and divisions. Therefore we obtain rational numbers.

AUDIENCE. Yes.

SERGE LANG. Look at an example. Somebody–you, madam, give me some value for t.

LADY. One half.

SERGE LANG. Thank you. We put $t = 1/2$ and we compute a little:

$$x = \frac{1 - 1/4}{1 + 1/4} = \frac{3/4}{5/4} = \frac{3}{5}$$

---

just like the one we have considered, and like we shall consider later. The search for these solutions is known today under the name of diophantine problems. The equations are called diophantine equations. See [Di], especially Book VI, where Diophantus solves problems concerned with Pythagorean triangles with additional conditions, using the formulas. See the end of the conference for the converse, and also [La–Ra]. Since it may interest people to see how Diophantus expressed himself, I reproduce here the first few lines of Problem XVIII of Book VI:

> To find a right triangle such that the number of its area augmented by the number of its hypotenuse forms a cube, and that the number of its perimeter is a square.
>
> If, as in the preceding proposition, we suppose that the number of the area is one arithme, and that the number of the hypotenuse is a cubic quantity of units, minus 1 arithme, then we are led to search for a cube which, augmented by two units, is a square . . .

There are about 300 pages in this style!

and

$$y = \frac{2 \cdot 1/2}{1 + 1/4} = \frac{1}{5/4} = \frac{4}{5}.$$

Here we find the triangle 3, 4, 5. OK, 1/2 is not very big and it is natural that we found the same solution in integers that we already knew. Now, if you want to do the computation with another fraction, maybe one that is not so simple, you will find other solutions. Do you want to give me another fraction?

LADY. 2/3.

SERGE LANG. All right, let's compute quickly:

$$x = \frac{1 - 4/9}{1 + 4/9} = \frac{9 - 4}{9 + 4} = \frac{5}{13}$$

$$y = \frac{2 \cdot 2/3}{1 + 4/9} = \frac{4/3}{13/9} = \frac{12}{13}.$$

Now we got back the solution 5, 12, 13 which somebody already mentioned. It's clear that you can continue with any fraction t, or any integer t. If you substitute for instance $t = 154/295$, you will get values for x and y which are a lot bigger, and which will give solutions. By this process, you see how to obtain an infinite number of solutions. It is a theorem that one obtains all of them except one: $x = -1$ and $y = 0$ cannot be obtained by such substitutions in the formulas. But all the other solutions (x, y) in rational numbers can be obtained by this procedure, by substituting a rational value for t in the formulas

$$x = \frac{1-t^2}{1+t^2} \quad \text{and} \quad y = \frac{2t}{1 + t^2}.$$

Since I want to deal with another topic at greater length, I am going to skip now the proof that this gives all the solutions except one of them. Maybe there will be time to give this proof later, after the talk.

MR. A. You said that one "sees" that there is an infinite number of solutions. Who "sees" it?

SERGE LANG. If you substitute an infinite number of values of t in these formulas, you get an infinite number of values of x.

MR. A. But it's not so easy to see.

SERGE LANG. Yes, it is, but I don't want to go into details now.

MR. A. But I want to say that it cannot be seen so easily. [*Brouhaha in the audience.*]

SERGE LANG. It depends who looks at it, it depends how good your eyes are. [*Laughter.*] [2]

OK, we just considered the equation $x^2 + y^2 = 1$. Suppose we want to generalize this equation, and study others which are more complicated. What will be the next complicated type of equation that we should look at? Let's pick on somebody. Madam.

THE LADY. Replace 1 by another number.

SERGE LANG. That's a possibility. We can study $x^2 + y^2 = D$. There is a theory for that which is quite similar to the one we have just seen. Let me skip it.

AUDIENCE. Look at the equation $x^2 + y^2 + z^2 = D$.

SERGE LANG. Very good, we can increase the number of variables. This raises some very interesting questions. But I am trying to make you say what I have in mind, I am trying to make you suggest what I intend to do.

AUDIENCE. Replace the square by a cube.

SERGE LANG. There we are. For example, the equation $x^3 + y^2 = D$, obtained by putting 3 instead of 2. Let's write it in the most classical form:

$$y^2 = x^3 + D.$$

For instance, $y^2 = x^3 + 1$. Are there infinitely many solutions? Is there even a single one?

AUDIENCE. Yes. 2 and 3, because $3^2 = 2^3 + 1$.

SERGE LANG. Is there another one?

AUDIENCE. $x = 0, y = 1$; and $x = -1, y = 0$.

SERGE LANG. OK, we now have three solutions. Is there another one?

AUDIENCE. $x = 0, y = -1$.

SERGE LANG. That's right, because of the square, we can take y or $-y$. So to summarize, we have the five solutions:

$$x = 0, y = \pm 1; \qquad x = -1, y = 0; \qquad x = 2, y = \pm 3.$$

---

[2] No matter how you look at it, you will find immediately what you are looking for. For instance, we have the equation

$$x(1 + t^2) = 1 - t^2 \qquad \text{so} \qquad (1 + x)t^2 = 1 - x \qquad \text{and} \qquad t^2 = \frac{1 - x}{1 + x}.$$

So to each value of x there corresponds a value of t or $-t$, and at most two values of t give the same value of x.

One can also notice that if t increases from 0 to 1 then $1-t^2$ decreases, while $1+t^2$ increases, so $x = (1-t^2)/(1+t^2)$ decreases from 1 to 0. In particular, different values of t give different values of x.

Are there other solutions? Who says yes? Raise your hand. Who says no? Who keeps a prudent silence?

It's not at all trivial. The difficulty to find solutions for this equation, and other similar ones, is much greater than for the equation $x^2 + y^2 = 1$. It is a theorem that there is no other solution. It's out of the question to prove it here.

Now, who knows about graphs? Do you know how to draw a graph? Who does not know? Raise your hand so I can see. [*A few hands go up.*] OK, I shall explain briefly what a graph is.

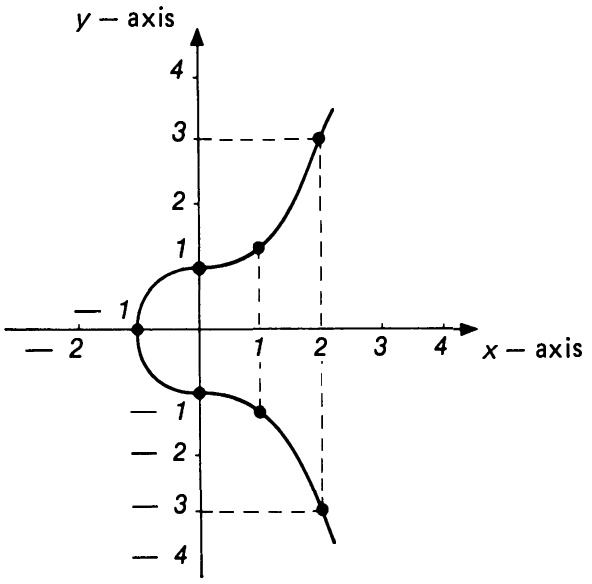
Suppose I have here on this axis values of x, and on the other axis values of y, and each x is a real number. For any real number x, I cube it, I add 1, and then I find two values for y:

$$y = \sqrt{x^3+1} \qquad \text{and} \qquad y = -\sqrt{x^3+1}.$$

For example:

if $x = 1$, then $y = \pm\sqrt{2}$;
if $x = 2$, then $y = \pm 3$;
if $x = 3$, then $y = \pm\sqrt{28}$;
if $x = -1$, then $y = 0$.

If x is negative and smaller than -1, then $x^3 + 1$ is negative, and there won't be a corresponding value for y. On the opposite side, if x grows indefinitely, then y grows also. To each x there correspond values y and $-y$, as on the following figure.



We can generalize our equation as you wanted to do earlier for $x^2 + y^2$, by considering

$$y^2 = x^3 + D, \quad \text{where } D \text{ is positive or negative.}$$

We also want to consider the equation $y^2 = x^3 + x$, or $y^2 = x^3 + ax$, which has considerable historical interest. For example, the Greeks and the Arabs had raised the following question. What are the rational numbers A such that A is the area of a right triangle, with integral sides a, b just like those we considered at the beginning. One can show that A is such a number if and only if the equation

$$y^2 = x^3 - A^2x$$

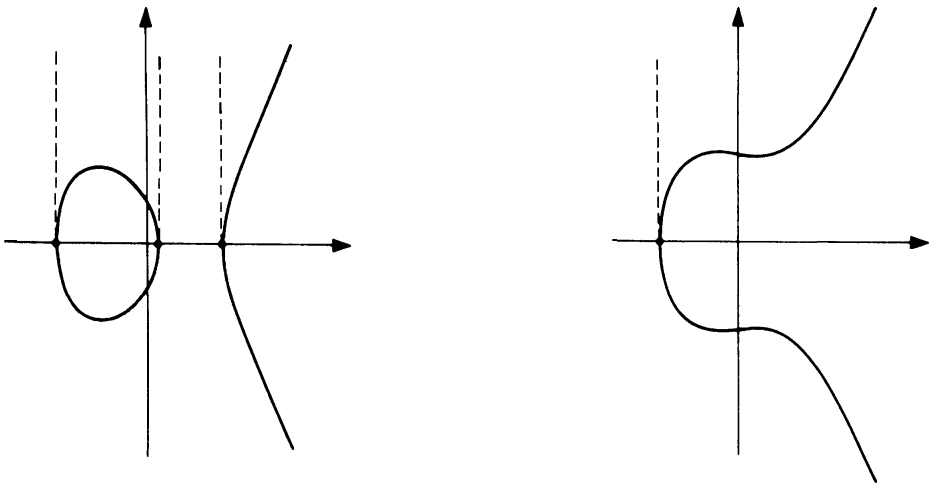
has infinitely many rational solutions.[3]

So finally, let's consider the equation

$$y^2 = x^3 + ax + b,$$

which covers all these cases. When we dealt with $y^2 = x^3 + b$ or $y^2 = x^3 + ax$, we assumed that $b \neq 0$ and $a \neq 0$, otherwise the equations are too degenerate. Similarly, for the general equation, we assume that $4a^3 + 27b^2 \neq 0$, to guarantee the appropriate non-degeneracy. For our purposes, you don't need to pay any more attention to such a technicality.

The graph of the general equation $y^2 - x^3 + ax + b$ is going to look like this, with a branch tending to infinity, and sometimes an oval.



[3] The area of a right triangle whose sides are a, b and hypotenuse c is given by the formula

$$A = ab/2.$$

Hence we find

$$c^2 + 4A = a^2 + b^2 + 2ab = (a + b)^2$$

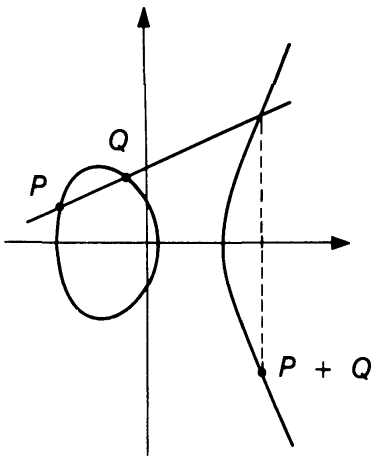
$$c^2 - 4A = a^2 + b^2 - 2ab = (a - b)^2.$$

It follows that a rational number A is the area of a right triangle if and only if one can solve simultaneously the equations

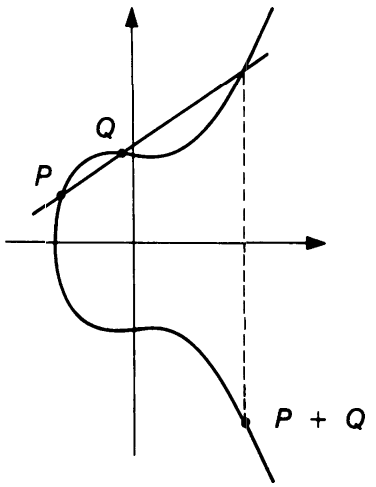
$$u^2 + 4Av^2 = w^2$$

$$u^2 - 4Av^2 = z^2$$

Using this graph, we can define an addition for points. Take two points P and Q on the curve. We define the sum of these two points in the following way. The straight line passing through P and Q intersects the curve in a third point. We reflect this point over the x-axis, and we find a new point which we denote by $P + Q$ as on the figure.



a) case where there is an oval



b) case where there is no oval

A UNIVERSITY STUDENT. But it does not always happen that the line through two points intersects the curve in a third point.

SERGE LANG. Oh yes? Can you give me an example?

A STUDENT. Well, yes, if the line is vertical.

SERGE LANG. Excellent remark. She is right, because if Q is the reflexion of P over the x-axis, then the vertical line will not cut the curve in any other point. We shall come back to this special situation in a moment. But this is essentially the only possible example of this phenomenon. Before looking at this special case, let's go back to the definition of the sum of two points.

I have used the symbol $+$. You have the right to expect certain properties, otherwise I should not have used the symbol $+$. What are those properties?

AUDIENCE. ???

---

in rational numbers (u, v, w, z). In a recent article, J. Tunnell [Tu] took up this theme and remarked that if one makes a projection from the point $(1, 0, 1, 1)$ onto the plane $z = 0$, then one obtains a correspondence between the curve defined by these simultaneous equations, and a plane curve, which itself can be put in the form

$$y^2 = x^3 - A^2x,$$

which is precisely of the type we are now considering. Tunnell gives criteria for the existence of an infinite number of solutions depending on recent, and quite difficult mathematical theories.

SERGE LANG. You know the symbol + from ordinary addition of numbers. I have just defined an addition of points. Which properties does addition of numbers have?

SOMEONE IN THE AUDIENCE. It's a group law.

SERGE LANG. Don't use such fancy language.

SOMEONE ELSE. The order of the terms can be reversed.

SERGE LANG. Indeed, that's the first property. We must have

$$P + Q = Q + P.$$

Which is true. To compute $Q + P$, I use the same straight line, so I find the same point of intersection, so the same sum $Q + P = P + Q$. What other properties can you expect?

SOMEONE IN THE AUDIENCE. Associativity.

SERGE LANG. You, it's clear that you know too much. [*Laughter.*] Let others speak too. For instance, the lady, there.

LADY. Associativity.

SERGE LANG. Yes, that's right. What does it mean? If I take the sum of three points, I could take it in two possible ways:

$$P + (Q + R) \qquad \text{and} \qquad (P + Q) + R.$$

Associativity means that these two expressions are equal, therefore we have

$$P + (Q + R) = (P + Q) + R.$$

It's obvious that $P + Q = Q + P$, but if you try to prove associativity, you won't find it so easy. If you try by brute force, you won't succeed. But it's true.

What other properties do you expect?

A HIGH SCHOOL STUDENT. A neutral element?

SERGE LANG. That's it. So what will be the neutral, or zero element? It means an element such that

$$P + \text{neutral element} = P.$$

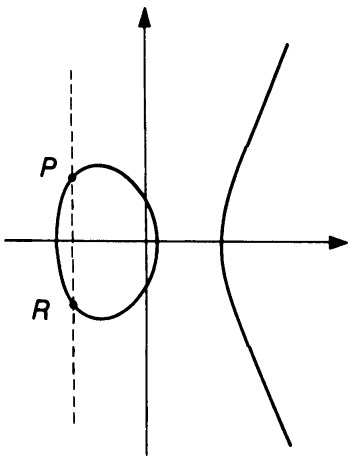
Is there one?

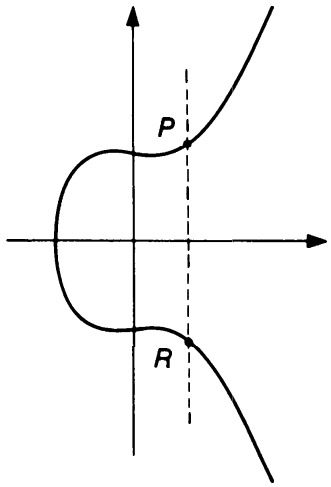
SOMEONE. The point over there.

SERGE LANG. No. This requires some imagination. Ah [*Laughing*] the gentleman over there does like this [*pointing upward.*] Are you a mathematician?

GENT. No, but I have been one. [*Laughter.*]

SERGE LANG. We are forced to invent this neutral element. Let's redraw the figure.





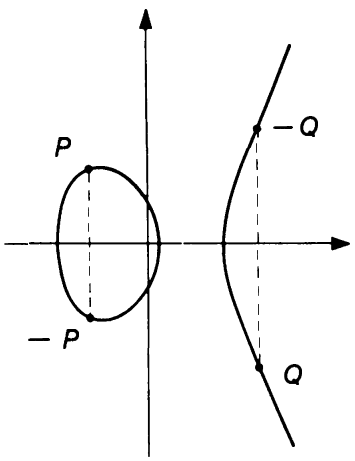
You are given a point P. What do I have to find? I must find something which is such that, when I take the straight line between P and this something, the line cuts the curve in a point whose reflection over the x-axis is P itself. The reflection of P is denoted by R in the figure, and the line passing through P and R is the vertical line. Consequently, if there is a point O such that $P + O = P$, this point cannot lie anywhere in the plane, because it must be on the curve and on the vertical line. So what do we do? We invent this point. We call it zero, and denote it by O. We say that O is at infinity. All the vertical lines tend toward infinity, going up or down. We make the convention that all these points at infinity are all the same point. We define a single point at infinity, which we view as the intersection of all vertical lines. It is a convention we accept that the straight vertical line passing through P also passes through P and O, and if this line cuts the curve at R, then $P + R = O$. Then what should we call R?

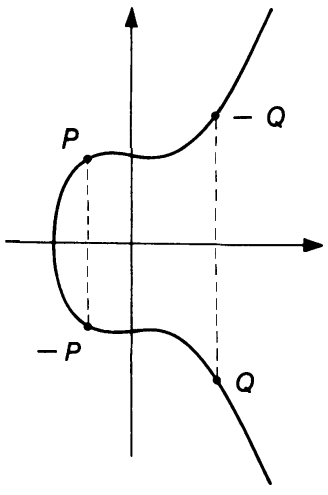
AUDIENCE. Minus P.

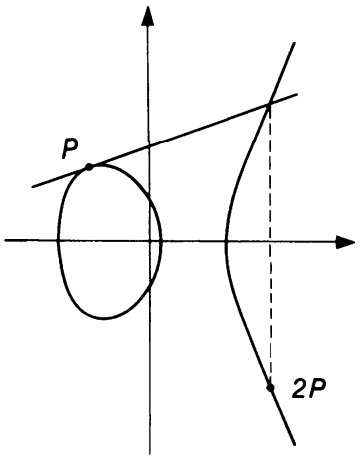
SERGE LANG. Yes, very good, because one has the condition

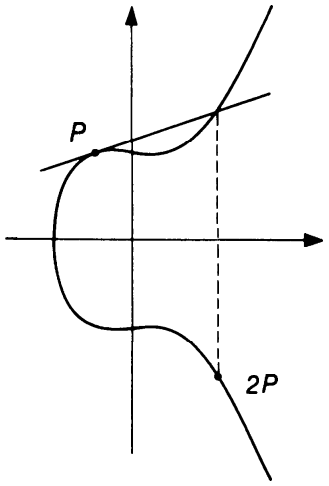
$$P + (-P) = O.$$

That's the convention we adopt.









And if I want to find $P + P$, what do I do?

AUDIENCE. Take the tangent.

SERGE LANG. That's right, perfect. The tangent to the curve at P cuts the curve in a point, which we reflect to obtain $P + P$, which I also denote by $2P$. Suppose I want to find $3P$. What do I do? I take the sum $2P + P$, always following the same process: I draw the line between P and $2P$, I reflect the point of intersection of this line with the curve, and I find $3P$. Same thing for

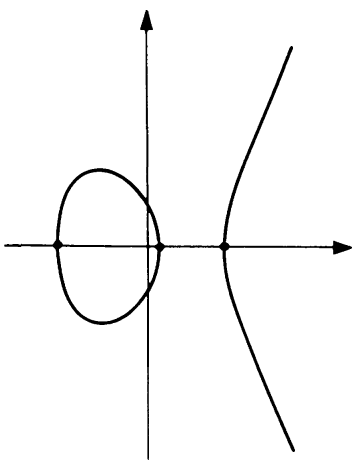
$$4P = 3P + P, \qquad 5P = 4P + P, \qquad \text{and so on.}$$

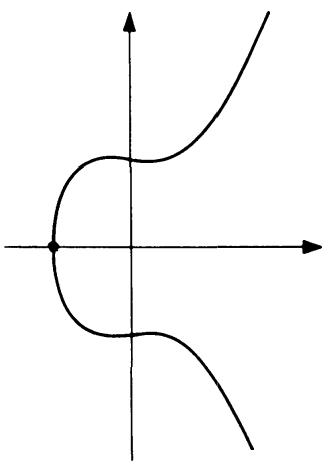
Now a little question. Where are all the points P such that $2P = O$? Use your imagination. Where are they? You. [*Pointing to someone.*]

SOMEONE. I don't see.

SERGE LANG. You saw how we find $2P$. We draw the tangent, we look at where the tangent cuts the curve, we reflect, and we get $2P$. Now I want $2P$ to be at infinity.

GENTLEMAN. On the horizontal line.





SERGE LANG. That's right, the points P such that $2P = O$ will be the points whose tangent is vertical, and therefore the points on the curve which lie on the horizontal line, the x-axis. There will be three such points if there is an oval. If there is no oval, then there is only one such point. Plus O itself, of course.

Suppose we have found a point $P = (x, y)$ which is rational, that is whose coordinates (x, y) are rational numbers.

Then in general, I can find other rational points: the multiples $2P$, $3P$, $4P$, etc. will also be rational. One can see this because one can give a formula for the addition of two points.

Let's look at three points on the curve $y^2 = x^3 + ax + b$:

$$P_1 = (x_1, y_1), \qquad P_2 = (x_2, y_2), \qquad P_3 = (x_3, y_3)$$

and suppose that $P_3 = P_1 + P_2$. How do you compute the coordinates x_3, y_3 from the coordinates x_1, x_2, y_1, y_2? There is a formula:

$$x_3 = -x_1 - x_2 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2.$$

Of course if $x_1 = x_2$ then the formula does not make sense. In this case, if $P = (x, y)$, then we compute $2P$ by the formula

$$x_3 = -2x + \left(\frac{3x^2 + a}{2y} \right)^2.$$

[*Six persons leave the audience at this point.*]

These formulas, again, nobody can find them just like that. They lie much deeper than those which give rational points on the circle. One needs serious ideas, general ideas, in order to arrive at the notion of straight line between two points intersecting the curve in a third point. But if you follow this procedure, and if algebra does not give you any trouble, then you will be able to derive these formulas with about a page of computations.

Let's apply these formulas to find rational points. We pick a concrete example, for instance the equation

$$y^2 = x^3 - 2.$$

There is a first solution, $x = 3$ and $y = 5$. Let's call this solution P. Then Mr. Brette (who organized the conference at the Palais de la Découverte),

was kind enough to do the computations with a computer, in order to find multiples of P. The solution $2P$ has coordinates $2P = (x_2, y_2)$ where

$$x_2 = \frac{129}{100} \quad \text{and} \quad y_2 = \frac{-383}{1000}.$$

He substituted $x = 3$ and $y = 5$ in the formula for $2P$. Then he went on to find the following table.

The curve $y^2 = x^3 - 2$
Multiples $nP = (x_n, y_n)$ of the point (3, 5)

n	x_n	length
1	3 1	1
2	129 100	3
3	164323 29241	6
4	2340922881 58675600	10
5	307326105747363 160280942564521	15
6	794845361623184880769 513127310073606144900	21
7	496803175045292277861 10937923 345851910470261667904471 9441	29
8	300370887246304508033820355385035059 21 301068398289876307178684299377991 8400	38
9	182386897568483763089689099250940650872600619203 127572396335305049740547038646345741798859364401	48
10	291678828031309584333972349170194008422407356276649505332 49 133299362853639218191065074976813043197323638166264832025 00	59
11	824172661141552804187727190037944704511772520763880755114120154630088 03 918020566047336292639939825980373481958168604589649639535939426806601	71

For reasons of space, the values of y_n are omitted. One can compute them by the formula

$$-y_3 = \left[\frac{y_2 - y_1}{x_2 - x_1}\right](x_3 - x_1) + y_1 .$$

If you look at the numerator of x_n in this table, you see that the numerators of these fractions increase very regularly. In fact, the way they increase has been one of the fundamental problems in this field of mathematics, diophantine equations. I have shown you the simplest example, after the equation of the circle.

The problem is to find all solutions, in integers or rational numbers, for equations of this type. It's extremely hard. There is no known procedure today to determine all the solutions. For the special equation

$y^2 = x^3 - 2$, I was able to write down one solution by inspection. But if I give you an equation of this type, there is no systematic method which allows you to find a first solutions, by an effective process. It's one of the great problems that mathematicians face: find a first solution by an effective process. But if I give you a first solution, then you can find others by applying the formulas.

Two cases can happen. The first is like the case with $2P = O$, but when, instead of $2P$, we might have $3P = O$, or $4P = O$, or $5P = O$. In general, if P is a point on the curve such that

$$nP = O$$

with some positive integer n, then we say that P is a point of finite order, or of order n. One question is to find out if there exist many rational points of finite order. One of the greatest discoveries of modern mathematics is due to Mazur, just three or four years ago [Maz], that if P is a rational point of order n, then n is at most 10, or $n = 12$. Furthermore, there are at most 16 rational points of finite order.[4]

The second case is when you construct $2P, 3P, 4P, \ldots$ you find a new point each time, like in the table a minute ago. You find points whose size grows regularly.

I am now going to show you, in the remaining few minutes, what are some of the theorems and conjectures concerning such equations and their solutions.

In 1922, Mordell [Mo] proved a conjecture of Poincaré [Poi] that one can always find a finite number of rational points

$$P_1, P_2, P_3, \ldots, P_r$$

such that any rational point P can be written as a sum of these points; this means that there are integers $n_1, n_2, \ldots, n_r$ depending on P, such that P can be written as a sum,

$$P = n_1 P_1 + n_2 P_2 + \cdots + n_r P_r.$$

Addition is, of course, addition on the curve as I have defined it.

[*Someone raises his hand.*]

SERGE LANG. Yes?

A HIGH SCHOOL STUDENT. What's "r"?

SERGE LANG. That's a very good question. There might be relations between the points $P_1, \ldots, P_r$. For example, one of them could be of finite

[4] Mazur's methods are among the most advanced of contemporary mathematics, and depend on what is called algebraic geometry and the theory of modular curves.

order. One can prove that we can always choose the points $P_1, \ldots, P_r$ such that any rational point can be expressed as a sum

$$P = n_1 P_1 + n_2 P_2 + \cdots + n_r P_r + Q,$$

with integers $n_1, \ldots, n_r$ which are uniquely determined by P; and Q is a point of finite order. This means that there are no relations among the points $P_1, \ldots, P_r$. If I choose r like that, then r is the maximum number of points among which there are no relations. Since Poincaré, r is called the rank of the curve. The problem is to determine r and to find the points $P_1, \ldots, P_r$.

Nobody knows how to do it in general. In special cases, one has methods which give a solution to the problem. Here is a table of Cassels for curves $y^2 = x^3 - D$, where D is an integer between -50 and $+50$. In each case, the rank is 0, 1, or 2. Cassels give the points P_1, P_2 as they arise [Ca]. [*You will find the table in an appendix.*]

For the general case, there exist very deep conjectures; one of them is due to Birch and Swinnerton-Dyer, two English mathematicians [B–SD]; it gives the rank in terms of very complicated objects associated with the equation. I cannot enter here into these considerations. But you can see how little we know, since nobody today knows an example when the rank is large, nor even an example when the rank is bigger than 10 (I think, it may be 12). Still, mathematicians conjecture that there are cases when the rank is arbitrarily large. Anybody can think about this problem: find a curve with an equation

$$y^2 = x^3 + D,$$

with D an integer, whose rank is bigger than 15, or 20, or 100, or arbitrarily large. We believe that such curves exist, but it's a great challenge to find them.

Recently, Goldfeld formulated the question somewhat differently [Go]. He considers curves

$$Dy^2 = x^3 + ax + b,$$

where a, b are fixed and D varies. Let's say D is an integer, $D = 1, 2, 3, 4$, etc. How does the rank behave for these values of D? For instance, how many integers D are there less than or equal to a number X for which the rank is 0, so for which there won't be any rational point except possibly a point of finite order? How many $D \leqq X$ are there for which the curve has rank 1? How many $D \leqq X$ are there for which the curve has rank 2? And so on. Goldfeld suggested that one should find a fairly regular behavior for rank 0 or 1; in fact he expects that the density of each should be one half for rank 0 and one half for rank 1. This means that approximately half the curves should have rank 0, and half of them should have rank 1, with perturbations which depend on much more complicated invariants of the curve. And there should be relatively few values of D for which the rank is bigger than 1.

It is a fundamental problem to give a quantitative answer to questions like that, and similar questions for curves like

$$y^2 = x^3 + D,$$

with D variable, or for the general family of curves $y^2 = x^3 + ax + b$ with a and b variable: for which values of a, b do we get rank 0, 1, 2, 3, 4, or any given integer as the rank. Since we don't even know whether there exist such curves with rank bigger than 10, we are far from knowing the answer, except possibly conjecturally.

Euh . . . that's a lot of algebra. I hope it wasn't too much. I just wanted to try, and see if I could make you understand this kind of problem that mathematicians raise. But I have been talking for an hour, so I'll stop and we'll see if there are any questions and if you have gotten anything out of all this.

The questions

SOMEONE. What is it good for?

SERGE LANG. I already gave the answer last year: it's good to give chills in the spine to a certain number of people, me included.[5] I don't know what else it is good for, and I don't care. But I speak for myself only. Like von Neumann said, one never knows whether someone is going to find another use for it. I was just trying to show you the kind of problem that excites us, or that excites me.

A HIGH SCHOOL STUDENT. This kind of problem is analogous to someone doing research in physics or electronics. They do experiments, but they don't know what they will find. It's like penicillin, for instance.

SERGE LANG. There is no universal answer, but your comment is very valid.

A GENTLEMAN. There is a question which interests me very much: it's the hyperdimensions of space. I hear that Lobatchevski found up to thirty-two dimensions. Do you believe that's a limit, or are there more?

SERGE LANG. I don't know what you mean by hyperdimensions.

GENTLEMAN. You don't know what hyperdimensions mean? Do you believe there are only three dimensions in space?

SERGE LANG. If you put the question that way [*Laughter*] then I can give, if not an answer, then at least an analysis of the question. You asked me: "Do you believe there are only three dimensions in space?" What do you mean by "space"? If by space you mean "that" [*Serge Lang shows the room*] then by definition there are only three dimensions. If you want more dimensions, then you accept to give the word "dimension" a more

[5] Not to speak of Diophantus . . .

general meaning, which is anyway the one which has been accepted long ago. Every time you can associate a number with a notion, you have a dimension, no matter what kind of notion you start from; in physics, mechanics, economics, or anything else. In mechanics, besides the three spatial dimensions, you can have speed, acceleration, curvature, etc. In economics, take for example the big businesses, oil companies, the sugar companies, steel, agriculture, etc. and their gross profits in 1981. For each company you get a number, and therefore a dimension; and in addition, of course, the number 1981 associated with time. Then you can have hundreds of dimensions like that.

By the way, if you look in the Encyclopoedia of Diderot, under "dimension", you will see that d'Alembert wrote the comments, and here is what he wrote:

> This way of considering quantities of more than three dimensions is just as right as the other; because algebraic letters can be seen as representing numbers, rational or not. I have said above that it was not possible to conceive more than three dimensions. A clever gentleman friend of mine believes that one could nevertheless view duration as a fourth dimension, and that the product of time by solidity would in some way be a product of four dimensions. This idea can be challenged, but it has, it seems to me, some merit, were it only that of being new. [Did]

Naturally, a friend of his, that's him, but he is being careful. He understood that the notion of dimension should not be restricted to space, but could be associated with any situation when you can associate a number. Time is only one example.

The rank of curves which we discussed before is another example. We can say that if a curve has rank r, then the rational points generate a space of dimension r.

SOMEONE. Does it help you in your theories to be able to use computers to find solutions, may be not all solutions, but some of them?

SERGE LANG. Yes, definitely. The Birch and Swinnerton-Dyer conjectures were based on experimental data from computers, as well as intuition and theoretical results. Historically, the rate of growth of the length of the multiples of one point could have been discovered by computers. More precisely, if you have a rational point $P = (x, y)$ on the curve, write $x = c/d$ where c is the numerator and d the denominator. Write

$$nP = (x_n, y_n) \qquad \text{with} \qquad x_n = c_n/d_n.$$

Then how fast does c_n grow? It is a theorem due to Néron that the length of c_n grows approximately like n^2. In the table of multiples of P, you can see this growth illustrated for $n \leqq 11$. To make more precise what we mean by "approximately", I need a more elaborate mathematical language. I would have to say that it is a quadratic function, up to a bounded function. I don't want to go into this now. One can write down a

more precise formula for the length, but it's much more difficult.[6] Here I merely stated an approximate behavior for the length.

SOMEONE. Is there some relation between the addition of points that you showed us, and the question of strange attractors?

SERGE LANG. Strange attractors in what, physics?

THE PERSON. Yes, systems of iteration which give certain kinds of curves.

SERGE LANG. Are you a physicist?

THE PERSON. Yes.

SERGE LANG. I don't know your physics and you don't know my elliptic curves. Maybe it's time we should get to know each other. I don't know an answer to your question, I don't know much physics. But it's possible. [*To the audience:*] Do you see, what's happening right now? I wrote certain formulas which struck a chord in the gentleman's mind. They suggested something to a physicist, by free association of ideas. That's how one does research. Two things can happen. Either nothing comes of it, or the gentleman will pursue the idea, which perhaps will give new relations between certain physical theories and the theory of so-called elliptic curves–of cubic equations. Maybe we'll know next year. The physicist might give a conference on those relations. That's what research is. But right now, I don't know the answer.

A GENTLEMAN. Can you tell us something of Fermat's great theorem?

SERGE LANG. Fermat's conjecture?

GENTLEMAN. Yes.

SERGE LANG. One can generalize the equation we looked at, for example, we can consider $x^3 + y^3 = 1$, or more generally

$$x^n + y^n = 1$$

where n is an arbitrary positive integer. What happens when n goes from 3 to 4?

SOMEONE. There are no solutions!

---

[6] Let us write x as a fraction, $x = c/d$ where c is the numerator and d the denominator. Define the height of the point to be

$$h(P) = h[x(P)] = \text{maximum of } \log | c |, \log | d | .$$

Néron's theorem states in particular that $h(nP) = q(P)n^2 + O(1)$, where $q(P)$ is a number depending of P, and $O(1)$ is a term bounded independently of n. The number $q(P)$ is called the quadratic form of Néron–Tate, because Tate gave a very simple proof for its existence. Mathematicians raise many questions about this number $q(P)$, for example whether it is a rational number or not. People believe it is not, unless P is of finite order. One can define a distance between two points P and Q by letting the square of this distance be $q(P - Q)$. The study of this distance constitutes one of the fundamental problems of the theory.

SERGE LANG. Sir, you know too much, it's cheating. Don't butt in. Besides, there are solutions:

$$x = 1, y = 0 \quad \text{and} \quad x = 0, y = 1.$$

[*Laughter.*] Are there others than those with $x = 0$ or $y = 0$? Who says yes? Who says no? Who does not know the answer? [*There are still some people who did not raise their hands.*] Who thinks that the answer is known? [*Laughter.*] Who thinks that the answer is not known? [*Several hands go up.*] Who knows that the answer is not known? [*Laughter.*]

In fact, the answer is not known. One knows the answer for a large number of values of n, but not in general. That's Fermat's problem:

> Are there solutions of $x^n + y^n = 1$ in rational numbers, other than with $x = 0$ or $y = 0$, when n is an integer > 2?

The answer is not known in general. One believes that the answer is no.

A HIGH SCHOOL STUDENT. Do people hope to know the answer some day?

SOMEONE ELSE. But Fermat said that he knew the answer!

SERGE LANG. Yes, Fermat said that[7] but one still does not know it. As for the question if one hopes to know the answer some day, what does it mean?

THE STUDENT. Does humanity hope to know the answer? Is it provable, or has it been shown to be unprovable?

SERGE LANG. No, it's an act of faith that it's provable. Mathematicians—euh, to be careful, all those I know—[*Laughter*] believe that it's provable. I think that if you raise an intelligent mathematical problem, there is an answer which will be found, some day.[8] That means, it suffices to think about the problem, and somebody will find the solution. Problems which are not solvable, that is, for which one can prove that they are not provable one way or another, are pathological cases, and I don't care about them. They don't occur when one "does mathematics". You have to look for them specifically.

SOMEONE. What's the definition of an intelligent problem?

SERGE LANG. No definition. [*Laughter.*]

The problems that you will meet, like that, it's an act of faith by mathematicians that you can try to solve them, and that you will succeed.

---

[7] More precisely, Fermat used to write comments in the margin of Diophantus' collected works. Next to the problem where Diophantus gives solutions of Pythagoras' equation $a^2 + b^2 = c^2$, Fermat wrote that he had a "marvelous" proof of the fact that for higher degree, there are no other solutions besides the trivial solutions, but the margin was too small to write down his proof.

[8] My use of the word "intelligent" is obviously idiotic, and the following sentences are deficient in that they don't take into account properly the choice which everyone makes concerning the subject of one's research.

That's all. One does not even think of the possibility that they are perhaps not provable. And if you think too much about that, then maybe you will do something else, but you won't do this kind of mathematics. It will prevent you from thinking.

But watch out! There are some problems which are somewhere in between, for example what is called the continuum hypothesis. It is the only counterexample that I can think of right now.

QUESTION. What is the continuum hypothesis?

AUDIENCE. Cantor . . .

SERGE LANG. Yes, let's talk a little about the continuum hypothesis. Last year, somebody got chills in the spine just to know whether the real numbers are denumerable. Take all the real numbers, the numbers on the number line, or in other words, all the infinite decimals, like

$$212.35420967185\ldots$$

You also have the positive integers 1, 2, 3, 4,. . . One says that a set is denumerable if you can make a list of all the elements of the set, with a first, a second, a third, and so on, so that you catch all the elements of the set, so that none is left out. Somebody last year asked me to prove that the real numbers are not denumerable, and I gave the proof.

Mathematicians, or Cantor, raised the following question. Between denumerable sets, those that you can enumerate like the integers, and the real numbers, are there sets whose cardinality is in-between; that is, sets which have more elements than the denumerable sets—so that you cannot enumerate them—but which have fewer elements than the real numbers? What does it mean, "fewer"? It means that you cannot establish a one to one correspondence between the real numbers and the elements of this set. The continuum hypothesis was that there does not exist any such sets, non-denumerable, but with "fewer" elements than the real numbers.

Considering the way we write the real numbers, as infinite decimals, they seemed so close to the rational numbers (which are denumerable), that it seemed reasonable to think that there was no set of intermediate cardinality.

SOMEBODY. Maybe someone is trying to find the answer?

SERGE LANG. Of course, that's why I said that it was a counterexample to the statement I made. There is no doubt that the question is intelligent. And the solution was found by somebody who did not get caught by the way the question was phrased. It's Paul Cohen.

QUESTION. What century?

SERGE LANG. Recent, about fifteen years ago. And the answer is that the question is meaningless. One can prove neither that there exists such a set, nor that there does not exist such a set. The answer is that, given the mathematical system with which we work today, which is sufficient for all our needs except this one, if you add as an axiom the positive answer to

the continuum hypothesis, then you still have a consistent system, the system will still be valid. And if you add as an axiom the negative answer to the continuum hypothesis, then again the system will also be consistent.

AUDIENCE. It's independent of the axioms you already have.

SERGE LANG. That's right. What I mean is that the questions was badly posed. It means that when you speak of "sets", you don't know what you are talking about. The ambiguity lies in the intuitive notion you have of a set. Everybody has some intuition of sets: a set is a . . . bunch of things. [*Laughter.*] To say a bunch of things, it's OK if you speak of all the real numbers; it's OK if you speak of all the rational numbers; it's OK if you speak of all the points on a curve; but if you speak of all sets simultaneously, of all the sets contained in the real numbers, then it's not OK, it does not work any more. That's what Paul Cohen's answer means: our notion of set is too vague for the continuum hypothesis to have a positive or negative answer. There remains that many mathematicians feel the need of an axiom which is psychologically satisfactory, and which would imply either the continuum hypothesis or its negation. This side of mathematics is interesting to some people. It does not really interest me personally. But I have to admit that it was worth seeing: a question which nobody thought could have an answer other than yes or no; and the guy who answered: you are all wet, there is no possible answer.

THE HIGH SCHOOL STUDENT. Is it possible that Fermat's conjecture is of this type?

SERGE LANG. What do you want me to answer? From my point of view, it's obvious what I am going to answer. It's not me that's going to say that it could be of the same type. No way.

Besides, there is an argument . . . [*hesitates*] if you succeeded in proving that Fermat's problem is unsolvable, then ipso facto you would have shown that the conjecture is true. Because if there was a counterexample, then with some big computer, some day someone would pull out the counterexample. But I hate this type of argument, and as far as I am concerned, I regard it as the normal state of affairs that some day, somebody will prove Fermat's theorem, or will prove that it is false.

QUESTION. And you personally, do you believe it is true or false?

SERGE LANG. [*Hesitates*] Well, it's true. There is no other solution besides $x = 0$ or $y = 0$. For the following reasons. We begin to understand the theory of such equations from a general point of view. There is a general conjecture of Mordell which I am going to describe.

Take an equation, for instance

$$y^3 + x^2y^7 - 312y^{14} + 2xy^8 - 18y^{23} + 913xy + 3 = 0.$$

This is what one calls a general diophantine equation. We ask in general: are there infinitely many solutions of this equation in rational numbers x, y? We have already seen two types of examples when there exist such

solutions. In the first example, we could express x as a quotient of two polynomials in a variable t, and y similarly, so that the equation was satisfied as an indentity of t. This is precisely what happened we used the formulas

$$x = \frac{1 - t^2}{1 + t^2} \qquad \text{and} \qquad y = \frac{2t}{1 + t^2},$$

and found that $x^2 + y^2 = 1$, an identity in t. Clearly (despite somebody's objections), you will get infinitely many solutions. That's one of the possibilities.

The other possibility is that you can get solutions of the equation from a cubic, with formulas

$$x = R(t, u) \qquad \text{and} \qquad y = S(t, u),$$

where t, u satisfy an equation $t^2 = u^3 + au + b$ having infinitely many solutions; and R, S are quotients of polynomials, with rational coefficients.

The first possibility is called genus 0, and the second is called genus 1.

Mordell's conjecture says this. Let $f(x, y) = 0$ be an equation, where f is a polynomial with integer coefficients. If you cannot reduce this equation to the case of genus 0 or genus 1 by formulas like the above, then the equation has only a finite number of rational solutions. That's the conjecture.

In a family of equations like Fermat's, with n variable, there should be very few solutions. One can even prove that for $n \geqq 4$, the equation $x^n + y^n = 1$ cannot be reduced to genus 0 or genus 1. According to Mordell's conjecture, Fermat's equation should have only a finite number of solutions in rational numbers x and y. Some people have done computations going quite far, maybe up to $n = 1{,}000{,}000$, and one knows that up to that point, there are no solutions other than the obvious ones with $x = 0$ or $y = 0$. And if what we feel is true, then there should not be any others for even bigger values of n, because such families should behave in a regular way. If one has not found solutions at the beginning, for n small, then there should not be any later, when n is large. That's the general intuition which directs us when we work on diophantine equations. Well, OK, it's a working hypothesis. One is always ready to backtrack if somebody shows that it's wrong. That's how mathematicians work: we make working hypotheses, we try to prove something, but we are always ready to accept any evidence that we are wrong, and that we have to start over again.

[*Someone raise his hand.*] And the computers, can't you do anything with them?

SERGE LANG. Oh, the computer, it has been used many times. It is with computers that people have shown that there were no solutions up to n approximately 1,000,000.

QUESTION. Sir, I have a question—there are problems which were solved first with restrictive hypotheses, and then better mathematicians could eliminate these hypotheses. But still, the first proofs used these hypotheses. Why?

SERGE LANG. When you try to solve a problem, you try first to solve special cases, and then try more general cases. The first ideas that you have might work only in the special cases. Maybe other ideas are needed in the more general cases. Who knows when these new ideas will come? Or even if they will come to one person and not another? Somebody publishes a first paper, then someone else relies on these first results, and obtains further results, publishing a second paper, but with some new ideas; and so forth until the general problem is solved. That's how one works. It does not mean that the mathematician who succeeds in eliminating the restrictive hypotheses is "better" than the other. Quite the contrary, the first mathematician might have shown much more imagination, and might have opened up a whole domain of research where nobody understood anything before. It may be that this first contribution will be admired much more than the following ones which, perhaps, merely developed the first one's program.

QUESTION. Let me change the subject a little. At the beginning of your talk, you alluded to the teaching of mathematics in France . . .

SERGE LANG. Everywhere, in the whole world.

QUESTION. The subject is of current interest. How do you see things in this direction? There seems to be a general problem.

SERGE LANG. How do I see things? I don't understand the question. It's too general.

A HIGH SCHOOL STUDENT. Do you think that mathematics should be taught like that, just for the beauty of it and not for applications to physics, or that at least until the end of high school, they should be turned towards physics, toward applications?

SERGE LANG. The way you phrase your question is too . . . exclusive. One does not prevent the other. It's obvious that the negation of one extreme does not imply an extreme on the opposite side. Do what . . . what comes naturally. Of course, there should be applications when teaching mathematics. But from time to time, you must also be able to say: OK, let's look at $x^2 + y^2 = 1$ and let's find all the rational solutions. Some will like it, some won't like it, but I know it's the sort of thing students like. I know it because I have talked about this problem to 15 and 16 year old kids several times, and they like it. They thought it was interesting. At the beginning of the talk, they know one solution, maybe some student knows another, maybe still another, but usually nobody knows any more. And then, after five minutes, we succeed in giving infinitely many! Listen, you would have to be really insensitive not to

react positively. [*Laughter.*] Well, OK, this does not mean that you should not also do applications.

QUESTION. When you are at Yale, do you have the same approach to teaching?

SERGE LANG. Same as what? Here? Yes, of course, like this. [*Serge Lang points to someone. Laughter.*] Naturally! How else do you want me to do it? Today, I was caught a little short, I picked a topic . . . I wanted to see just how far I could go in doing mathematics with you. It was hard. Because I needed algebraic formulas, it's dangerous for a Saturday afternoon audience. [*Laughter.*] Don't think I was not conscious of the difficulty. [*Allusion to the six persons who left after the first formulas.*] I just wanted to see how it would go. It did not go so badly.

AUDIENCE. No, no!

SERGE LANG. Were it only, for instance, him, or him [*pointing*], or the physicist over there. It's clear that they got something out of it, each one something different. Even if there had been only these three, it was worth it, and there were many others. Even if some of you are hung up on the formulas, if you are still sitting here, nobody is forcing you.[9]

QUESTION. Is there any hope to solve the great mathematical problems which have not yet been solved?

SERGE LANG. That's what mathematicians do, research. They hope to solve the problems which have not yet been solved. If they did not have that hope, they would not be, by definition, mathematicians doing research.

QUESTION. But you also find problems?

SERGE LANG. Yes, of course. To find the problem of which one is going to work, on which I am going to concentrate, is at least as important as solving it. To do mathematics, it is also to find problems, to make conjectures. For example, following Goldfeld, I raise the problem of finding the asymptotic behavior of the rank in a family of curves

$$y^2 = x^3 + D,$$

for example when D varies, for a given rank > 1. The density should be 0, but maybe there is an asymptotic behavior, so bounded from below, which would be much stronger than simply finding curves with arbitrarily high rank.

QUESTION. Perhaps in teaching mathematics, at least at the beginning, there is too much emphasis on solving problems instead of showing

---

[9] At the beginning of the talk, the room was about full, with about 200 persons. During the question period, about half remain.

how to pose problems. That's why I come back on what you have said; some people have suggested modelization, or similar things in applied mathematics. It's very positive: ask questions related to simple problems, before starting to solve them. Perhaps that is where the teaching of mathematics is deficient.

SERGE LANG. There is no single place where it is deficient, there are always several. If you show me the books, I'll tell you concretely from the books. I cannot give a general recipe, just like that. I like to deal with concrete instances. I'll show you in the book what I think is deficient in itself. There are always many deficiencies depending on the teacher, depending on the class, depending on a whole lot of circumstances, internal and external. No matter what I said, I did not mean that there was a single reason or a single condition which caused the deficiencies.

QUESTION. Perhaps it would be useful to enumerate these deficiencies.

SERGE LANG. Maybe, but after that, one would have to . . . Listen, I wrote up last year's talk. It's right here. This is what I have to say. I said it, I did it. I am doing it again this year, the conference will again be published. You see how I express myself, how I do mathematics. It's serious business. But it does not mean that someone else should do exactly as I do, just this way. Different people react differently. Do as you like, after all. My point of view is never exclusive. I speak only for myself, I don't like generalizations.

A HIGH SCHOOL STUDENT. I am a high school student, and there is something which I object to in the teaching of mathematics.

SERGE LANG. What year?

STUDENT. 11th grade. And since I was very small, I was shown proofs, but I was not shown, to use your analogy with music, the beauty in them. There was no taste to what was done in school. When one does music, then one gets into the beauty of the music, not just its rythm, or the theory of music . . .

SERGE LANG. In any case, the beautiful proofs, they are not in the curriculum. There is a whole lot of beautiful ones, and usually they are omitted. But anyway, did you like what I did today, these structures, the diophantine equations?

STUDENT. Yes.

SERGE LANG. Are you into computers?

STUDENT. Yes.

SERGE LANG. Where, here?

STUDENT. No, in my school, in the suburbs. But if you want, I think a priori that people who would be exposed just like that to what you did today, they might not see the beauty in it, anyway not everybody.

SERGE LANG. Of course, in an aesthetic situation, there are some who see it right away, there are some who see it later, and there are some who never see it. This is typical of an aesthetic situation. I don't ask everybody to find what I did beautiful. But still, the formula we had,

$$x_3 = -x_2 - x_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2,$$

it's a little complicated, but the fact that it can give you infinitely many solutions for the equation, I find it fascinating. I don't know what you think, but you asked enough questions to show that you are reacting positively.

THE PHYSICIST. It seems that in French schools, the main reason for the heavy-handedness and lack of understanding is that, behind the whole program, one tries to show, even to very young children, a logical construction which is completely irrefutable. Whether it is in physics or mathematics, a teacher can never allow himself to assert something without giving a clear proof for it.

SERGE LANG. I entirely agree with this evaluation, and I deplore it as much as you do. It is true that the textbooks tend toward a certain aridity and are pedantic. I have nothing else to say.

A UNIVERSITY STUDENT. I am a student, but those problems, we see them, but we don't have time to deal with them. If we did, then we would still be at the beginning when we get to be forty years old.

SERGE LANG. But nobody asks you to do that the whole year long. When you go to a concert, nobody asks you to do music all the time till you are forty.

THE STUDENT. During math class, we see interesting problems, but if we go deeper into them, we spend hours and hours, and there is a lot of other things to do. The curriculum is much too heavy to allow us to take an interest in things like that.

SERGE LANG. It depends on the level. I think the curriculum is filled with stuff that could easily be taken out without anybody missing it. [*Laughter.*]

STUDENT. Can you tell me which ones?

SERGE LANG. Bring me the book and I'll show you. You can find more and more technical exercises, which don't teach anybody anything.[10]

---

[10] Here I misunderstood. I am speaking of elementary and high schools. Beyond, that is at the student's level, the situation is different, and complicated in different ways. I sympathize with what he said, but this is not the time to go into the contradictory requirements of education at the college level.

[*The preceding dialogue is extracted from a long general discussion—too general—on teaching. I pass now to my last answer.*]

I spend my life doing mathematics. From time to time, I do mathematics with you, just like this. I prefer to do this than to have general discussions. I prefer to come here, give this talk, show you how I teach, point my finger at you, and make you ask questions . . . and if it works, that was one of the ways of doing things. Maybe in this way, you will find your own inspiration, to do as you want to touch others. That's how I function, rather than by pontificating with generalizations. I don't like generalities. This does not mean that I never generalize, sometimes I do, but I don't like them.

There is some success in what I did today, for instance [*showing the high school student*] what's you name?

STUDENT. Gilles.

SERGE LANG. Gilles is one of those who asked questions on the mathematics. Others took refuge in pedagogical questions. I prefer Gilles' questions.

ANOTHER HIGH SCHOOL STUDENT. [*Antoine, who had also come last year.*] You told us that the formulas

$$x = \frac{1 - t^2}{1 + t^2} \qquad \text{and} \qquad y = \frac{2t}{1 + t^2}$$

give all the rational solutions of $x^2 + y^2 = 1$, except $x = -1$ and $y = 0$. Can you give us the proof now?

SERGE LANG. Yes, naturally, I had even hoped somebody would ask that question earlier. The proof is easy. Suppose that (x, y) is a rational solution. Let

$$t = \frac{y}{x + 1};$$

and don't ask me where it came from, with a little ingenuity you could discover it yourself.[11] We then have

$$t(x + 1) = y,$$

and squaring, we find

$$t^2(x + 1)^2 = y^2 = 1 - x^2 = (1 + x)(1 - x).$$

---

[11] G. Lachaud informs me that Diophantus, and therefore the Greeks, had not raised the question whether the formulas give all the solutions. He also informs me that this result is due to the Arabs of the 10th or 11th century [La–Ra]. The algebra necessary to prove this result is approximately at the same level as the algebra used by Diophantus, and so we see a posteriori that once the question is raised, one finds the answer rather easily.

You can then cancel $x + 1$ on both sides, and we find

$$t^2(x + 1) = 1 - x.$$

Therefore $t^2x + t^2 = 1 - x$, and

$$x(1 + t^2) = 1 - t^2.$$

Divide both sides by $1 + t^2$ to find the formula

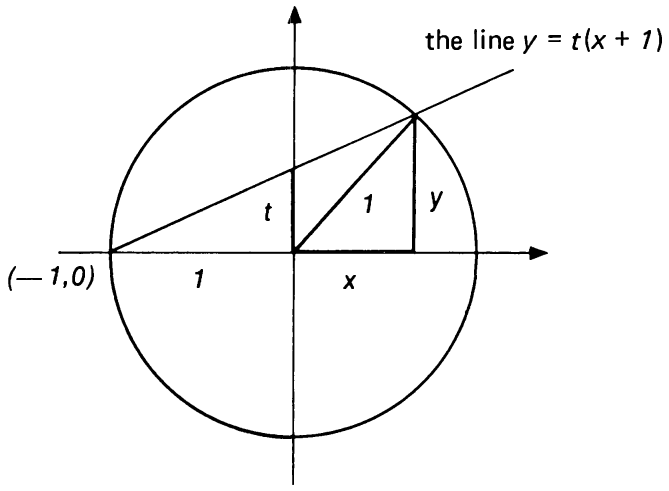
$$x = \frac{1 - t^2}{1 + t^2}.$$

One more line will give you the corresponding formula for y.

You can interpret the argument geometrically, thanks to ideas which appeared only in the 17th century, namely coordinates and the representation of equations by curves. Namely, $y = t(x + 1)$ is the equation of a straight line, passing through the point $x = -1$, $y = 0$; and whose slope is equal to t. This line intersects the circle of radius 1 at the point (x, y) such that

$$x = \frac{1 - t^2}{1 + t^2} \quad \text{and} \quad y = \frac{2t}{1 + t^2},$$

which is precisely what we have just shown.



I would like to add a few words on the difference between integral and rational solutions. We have seen that an equation like

$$y^2 = x^3 + ax + b$$

can have an infinite number of rational solutions, obtained as multiples nP of some rational point P. For instance, in the example

$$y^2 = x^3 - 2,$$

we started with the integral point $P = (3, 5)$. One can prove that it is the only integral point on the curve. Furthermore, there exists a very general theorem of Siegel, which says that the number of integral points on a curve $y^2 = x^3 + ax + b$ is always finite [Sie].

When a, b are integers, then any point of finite order (x, y) must necessarily be an integral point, that is x, y are integers, according to a theorem of Lutz–Nagell. Of course, the converse is false, as in the example with $x = 3$, $y = 5$ which is not of finite order.

By the way, about points of finite order, let me give you an easy exercise. Go back to the curve $y^2 = x^3 + 1$. We found the integral points:

$$x = 0, y = \pm 1; \qquad x = 2, y = \pm 3; \qquad x = -1, y = 0.$$

I told you that there were no other rational points. It follows that if you take any one of these points, for instance $P = (2, 3)$, one of the multiples nP with a suitable n, must give O. So I ask you to compute explicitly $2P$, $3P$, $4P$, $5P$. It's easy with the addition formulas, and you can also do it on the graph. You will find all the other integral points, and you will also find that

$$5P = -P.$$

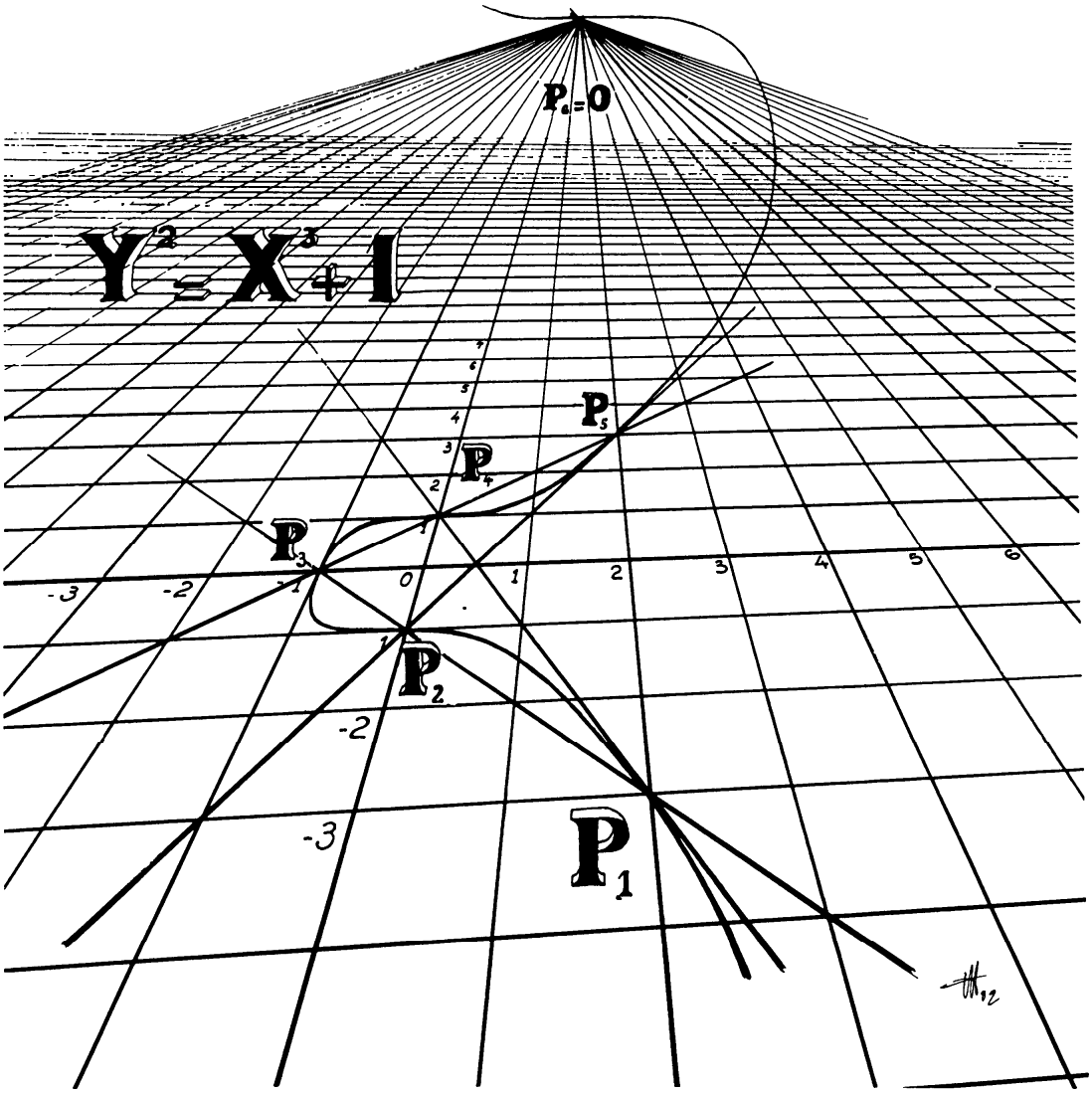
Therefore $6P = 5P + P = O$, and the point P has order 6.[12]

MR. BRETTE. [*Question asked two days later.*] You said that the order of a rational point is at most equal to 12. But if you look at all real points, does there exist points of arbitrary order?

SERGE LANG. Yes, and one can even describe them quite precisely. Suppose first for simplicity that there is no oval. Then for each integer $n \geqq 2$, there exists one point P of order exactly n (that is, P does not have smaller order), and such that every point of order n is equal to an integral multiple of P. If there is an oval, then the situation is the same, up to a point of order 2.

---

[12] I thank Mr. Brette for having drawn a very effective illustration of the curve (on the opposite page), which shows very clearly the point at infinity, and the rational points of finite order. Note that P_1 has order 6, P_2 has order 3, and P_3 has order 2.



Added August 1982

Following the talk, I continued to think about the determination of integral and rational points, to try to get more coherent conjectures about them. Siegel's proof did not give an upper bound for the integral points, depending on the coefficients a and b of the curve

$$y^2 = x^3 + ax + b.$$

We now suppose that a, b are integers. In the special case $y^2 = x^3 + b$, Baker [Ba] has given effective bounds, although far from the best possible ones which one might expect. For example, there is a conjecture of Marshall Hall which says that when b is an integer, then x is bounded in

absolute value by b^2 times some constant, independent of b.[13] I think one might expect something similar in the general case. It would be very interesting to show that there is some constant k such that for any integral point (x, y), the integer x is bounded in absolute value by a constant times the maximum of the absolute values of a^3 and b^2 raised to the kth power. One can write this in the form

$$| x | \leqq C \max (| a |^3, | b |^2)^k.$$

Finding bounds like that would constitute great progress in the study of such curves.

It would also be interesting to find bounds in the context of points of infinite order. More precisely, let $P = (x, y)$ be a rational point. Write $x = c/d$ as a fraction as we already have done. Define the height

$$h(P) = \log \max (| c |, | d |).$$

Considerations having to do with the Birch–Swinnerton–Dyer conjecture have led me to the following conjecture, understandable by someone who is not necessarily a number theorist. There exist points $P_1, \ldots, P_r$ as we have considered them previously, ordered by increasing height, such that

$$h(P_r) \leqq C^{r^2} \max (| a |^3, | b |^2)^{1/12 + \epsilon}$$

where C is some constant, and ϵ approaches 0 as $\max (| a |^3, | b |^2)$ increases indefinitely. See [La 2].

The existence of such bounds would allow an effective way of finding all the rational points, since these can be expressed by means of addition and subtractions starting with $P_1, \ldots, P_r$ and points of finite order.

Note that in tables, for instance that of Cassels or Selmer [Se], it seems that there is a better bound than that described above. If we let

$$H(P) = \text{maximum of } | c | \text{ and } | d | ,$$

then one has an approximate inequality

$$H(P) \leqq \max (| a |^3, | b |^2)^k$$

with $k = 1$, 2, or 3. I give a numerical example taken from Selmer's table, where he considers the related equation

$$X^3 + Y^3 = DZ^3$$

---

[13] Recall that the absolute value of a number is the positive part of the number. For example, the absolute value of -3 is 3, and the absolute value of -3 is 3 also. The absolute value of x is denoted by $| x |$.

as in Fermat's equation. Mr. Brette used the computer to transform Selmer's biggest solutions back to the form we have considered, that is

$$y^3 = x^3 + 2^4 3^3 D^2$$

with $b = 2^4 3^3 D^2$.

Take $D = 382$. Then we have a solution $x = u/z$, where

$$u = 96,793,912,150,542,047,971,667,215,388,941,033$$
$$z = 195,583,944,227,823,667,629,245,665,478,169.$$

The reader can compare this solution with b^2. You will find that $u \leqq b^6$, so $k = 3$ works. It would be interesting to make a statistical analysis of such polynomial bounds, rather than the logarithmic bounds conjectured previously.

Appendix

I reproduce below a table of Cassels [Ca]. The following comments will describe the content of the table, and how to read the columns.

Given a curve

$$y^2 = x^3 - D \qquad \text{with} \qquad -50 \leqq D \leqq 50,$$

we look for rational points $P_1, \ldots, P_r$ on the curve such that for every rational point P, there exist integers $n_1, \ldots, n_r$ uniquely determined by P, such that

$$P = n_1 P_1 + \cdots + n_r P_r + Q,$$

where Q is a point of finite order. Therefore, r is the rank.

In all cases, we have $r = 0$, 1, or 2. For instance, let

$$P_1 = (x, y).$$

Rather than make a table of rational numbers, we prefer integers. So we express the rational numbers x, y as fractions,

$$x = u/t^2 \qquad \text{and} \qquad y = v/t^3$$

with integers u, v, t. The equation of the curve can be expressed in terms of u, v, t in the form

$$v^2 = u^3 - Dt^6.$$

"None" means that the rank is equal to 0, and so the only rational points are of finite order, if there are any.

The first column gives P_1 if it exists.

The second column gives P_2 if it exists, besides P_1.

Table 1

$v^2 = u^3 - Dt^6$

D	P_1			P_2		
	u	v	t	u	v	t
1		None				
2	3	5	1			
3		None				
4	2	2	1			
5		None				
6		None				
7	2	1	1			
8		None				
9		None				
10		None				
11	3	4	1	15	58	1
12		None				
13	17	70	1			
14		None				
15	4	7	1			
16		None				
17		None				
18	3	3	1			
19	7	18	1			
20	6	14	1			
21	37	188	3			
22	71	119	5			
23	3	2	1			
24		None				
25	5	10	1			
26	3	1	1	35	207	1
27		None				
28	4	6	1			
29	3,133	175,364	3			
30	31	89	3			
31		None				
32		None				
33		None				
34		None				
35	11	36	1			
36		None				
37		None				
38	4,447	291,005	21			
39	4	5	1	10	31	1
40	14	52	1			
41		None				
42		None				
43	1,177	40,355	6			
44	5	9	1			
45	21	96	1			
46		None				
47	12	41	1	63	500	1
48	4	4	1			
49	65	524	1			
50	211	3059	3			

Table 1 (cont.)

$v^2 = u^3 - Dt^6$

D	P_1			P_2		
	u	v	t	u	v	t
−1		None				
−2	−1	1	1			
−3	1	2	1			
−4		None				
−5	−1	2	1			
−6		None				
−7		None				
−8	2	4	1			
−9	−2	1	1			
−10	−1	3	1			
−11	7	19	2			
−12	−2	2	1			
−13		None				
−14		None				
−15	1	4	1	109	1,138	1
−16		None				
−17	−1	4	1	−2	3	1
−18	7	19	1			
−19	5	12	1			
−20		None				
−21		None				
−22	3	7	1			
−23		None				
−24	−2	4	1	1	5	1
−25		None				
−26	−1	5	1			
−27		None				
−28	2	6	1			
−29		None				
−30	19	83	1			
−31	−3	2	1			
−32		None				
−33	−2	5	1			
−34		None				
−35	1	6	1			
−36	−3	3	1			
−37	−1	6	1	3	8	1
−38	11	37	1			
−39	217	3,107	2			
−40	6	16	1			
−41	2	7	1			
−42		None				
−43	−3	4	1	57	2,290	7
−44	−2	6	1			
−45		None				
−46	−7	51	2			
47	17	89	2			
−48	1	7	1			
−49		None				
−50	−1	7	1			

Bibliography

[Ba] A. BAKER, "Contributions to the theory of Diophantine equations II: The Diophantine equation $y^2 = x^3 + k$", *Phil. Trans. Roy. Soc. London* **A 263** (1968), pp. 173–208.

[B–SD] B.J. BIRCH and P. SWINNERTON-DYER, "Notes on elliptic curves I." *J. Reine Angew. Math.* **212** (1963), pp. 7–25.

[Ca] J.W. CASSELS, "The rational solutions of the diophantine equation $y^2 = x^3 - D$," *Acta Math.* **82** (1950), pp. 243–273.

[Did] DIDEROT, article "Dimension", *Encyclopédie* Vol. 4 (1754), p. 1010.

[Di] DIOPHANTE D'ALEXANDRIE, *Les six livres arithmétiques et le livre des nombres polygones*, Paul ver Eecke, Albert Blanchard, Paris 1959.

[Go] D. GOLDFELD, "Conjectures on elliptic curves over quadratic fields," à paraître.

[Ha] M. HALL, "The diophantine equation $x^3 - y^2 = k$," *Computers and Number Theory*, Academic Press, 1971, pp. 173–198.

[La–Ra] G. LACHAUD and R. RASHED, Une lecture de la version arabe des "Arithmétiques" de Diophante; cf. les *Oeuvres de Diophante*, Collection Guillaume Budé, Les Belles Lettres, Paris, 1984.

[La 1] S. LANG, *Elliptic Curves: Diophantine analysis*, Springer-Verlag, 1978.

[La 2] S. LANG, "Conjectured diophantine estimates on elliptic curves," in a volume dedicated to Shafarevich, Birkäuser, Boston–Basel, 1983.

[Ma] B. MAZUR, "Modular curves and the Eisenstein ideal," *Pub. Math. IHES*, 1978.

[Mo] L.J. MORDELL, "On the rationnal solutions of the indeterminate equation of the third and fourth degrees," *Proc. Camb. Phil. Soc.* **21** (1922) pp. 179–192.

[Ne] A. NERON, "Quasi-fonctions et hauteurs sur les variétés abéliennes," *Ann. of Math.* **82**, No. 2 (1965), pp. 249–331.

[Poi] H. POINCARÉ, "Arithmétique des courbes algébriques," J. de Liouville, 5^e série, t. VII, fasc. III (1901), pp. 161–233, Oeuvres complétes, t. V, Gauthier-Villars, 1950.

[Pod] V.D. POSDIPANIN, "On the indeterminate equation $x^3 = y^2 + Az^6$," *Math Sbornik*, **XXIV** (66), No. 3 (1949), pp. 392–403.

[Si] C.L. SIEGEL, "The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$," *J. London Math. Soc.* **1** (1926), pp. 66–68 (under the pseudonym **X**).

[Tu] J.B. TUNNELL, "A classical diophantine problem and modular forms of weight 3/2." *Invent. Math.* (1983) pp. 323–334.

[vN] J. von NEUMANN, "The role of mathematics in the sciences and in society," address to Princeton Graduate Alumni, *Complete works*, vol. VI, pp. 477–490.