To be Published in *The Special Issue of The Proceedings of Telangana Academy of Sciences*
Vol. 00, No. 00, 2020, 1–10

Diophantine Equations An Introduction

Dinakar Ramakrishnan*

California Institute of Technology

(*Received 00 Month 20XX; final version received 00 Month 20XX*)

Abstract: This is a redaction of the Inaugural Lecture the author gave at the University of Hyderabad in January 2019 in honor of the late great Geometer (and Fields medalist) Maryam Mirzakhani.

What is presented here is a limited perspective on a huge field, a meandering path through a lush garden, ending with a circle of problems of current interest to the author. No pretension (at all) is made of being exhaustive or current.

1. Something light to begin with

When Nasruddin Hodja claimed that he could see in the dark, his friend pointed out the incongruity when Hodja was seen carrying a lit candle at night. "Not so," said Nasruddin, "the role of the light is for others to be able to see me."

The moral is of course that one needs to analyze all possibilities before asserting a conclusion.

Maryam Mirzakhani, whom this Lecture is named after, would have liked the stories of Hodja.

Mirzakhani's mathematical work gave deep insights into the structure of geodesic curves on hyperbolic surfaces. Such surfaces also play a major role in the field of Number theory, often through an analysis of Diophantine equations.

Etymology: *Hod* (or *Khod*) is of Persian origin meaning *God*, and 'Hodja' serves God, signifying a Mullah, Priest, Rabbi, Minister or Pundit (depending on one's favorite religion).

The expression *Khoda Hafez* (or 'Khuda Hafiz' in Urdu) of course means 'May God protect you' or just 'Goodbye' in the modern usage.

Hafiz is of Arabic origin meaning 'protector'.

2. A basic Definition

By a **Diophantine equation**, one means an equation of the form

$$f(X_1, X_2, \ldots, X_n) = 0$$

*Corresponding author. Email: dinakar@caltech.edu

where f is a polynomial (in n variables) with *coefficients in the ring of integers* $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots, \pm n, \dots\}$. Denote as usual by $\mathbb{Q}$ the field of rational numbers.

One wants to find integral (or rational) vectors $x = (x_1, \dots, x_n)$ such that $f(x) = 0$.

A study of these equations was initiated by *Diophantus of Alexandria*, who lived in the third century AD. He wrote a series of books titled *Arithmetica*, whose translation into Latin by Bachet influenced many including Pierre de Fermat. See [D], which gives a link to an English translation, and [Sch] which links to an interesting essay on Diophantus.

Diophantus may have lived earlier, and a key commentary on him by *Hypatia* is missing. Also one of Diophantus's works is missing, as he quotes some Lemmas from there in *Arithmetica*.

The consensus seems to be that he was Greek. He was likely well versed in Ancient Greek, as many learned people probably were in Alexandria, but could he have been Egyptian (or Jewish or Caldean)?

Of particular interest ar *homogeneous* Diophantine equations, i.e., with $f(x_1, \dots, x_n) = 0$ with f a homogeneous polynomial. In this case, any integral solution $a = (a_1, \dots, a_n)$ leads to infinitely many integral solutions $(ba_1, \dots, ba_n)$ as b varies in $\mathbb{Z}$. One calls the solutions *a primitive* if the gcd of $\{a_1, \dots, a_n\}$ is 1.

More generally, one may consider *Diophantine systems*, which are finite collections of Diophantine equations, and look for *simultaneous* integral (or rational) solutions.

3. Pythagorean triples

These are (positive) Integral Solutions of $X^2 + Y^2 = Z^2$.

The first sixteen primitive Pythagorean triples are
$(3, 4, 5), (5, 12, 13), (8, 15, 17), (7, 24, 25), (20, 21, 29), (12, 35, 37),$
$(9, 40, 41), (28, 45, 53), (11, 60, 61), (33, 56, 65), (16, 63, 65),$
$(48, 55, 73), (36, 77, 85), (13, 84, 85), (39, 80, 89),$ and $(65, 72, 97)$.

A larger triple is $(403, 396, 565)$.

Many old civilizations (in Babylon, China, India, for example) studied this equation long before Pythagoras. The Babylonians even found the non-trivial triple $(3367, 3456, 4825)$.

All primitive solutions can in fact be *parametrized* by:
$(2mn, m^2 - n^2, m^2 + n^2)$, $m > n$, with
m, n of opposite parity, $(m, n) = 1$.

To get at this, one looks for rational solutions of $u^2 + v^2 = 1$, which are geometrically realized as **rational points** on the unit circle S.

They are obtained by intersecting S with secant lines with rational slope emanating from $(-1, 0)$.

This illustrates the basic idea of embedding rational solutions inside real, or complex, points of the *variety* V defined by the diophantine equation $f(x) = 0$.

Once we have the rational solutions (u, v) of $u^2 + v^2 = 1$, one can clear the denominators and get integral solutions of $x^2 + y^2 = z^2$. A bit more work yields all the primitive Pythagorean triples.

A quick subjective comment. The approach of the Greeks in such problems stressed the importance of a proof (of completeness), which forms the basis of modern mathematics, while that of the earlier ones was more algorithmic.

4. $X^2 - dY^2 = 1$

Fermat's challenge of 1657 to find an integral solution for $d = 61$ brought this equation, attributed to Pell, to prominence.

However, three centuries earlier, Bhaskara in India had derived the solution $(1766319049, 226153980)$
using the **Chakravaala Vidhi** (*Cyclic method* or 'rule') due to him and (earlier) Jeyadeva.

This method provided an *algorithm* to construct from one solution many other solutions, infinitely many, and one gets all solutions this way, though there was no proof at that time.

In fact, already in the seventh century, Brahmagupta had solved this equation for $d = 83$. He derived a composition law and also 'shortcuts' like going from a solution of $u^2 = dv^2 = -4)$ to $u^2 - dv^2 = 1$; for $N = 61$, $39^2 - 61(5^2) = -4$.

For an instructive and beautiful discussion of this method of the Indian mathmaticians of olden times, see [We].

5. Sums of three squares

Diophantus investigated the representation of a positive integer n as a sum of three squares, i.e., looked at the equation

$$X^2 + Y^2 + Z^2 = n.$$

For $n = 10$, he found the elegant solution in positive integers:

$$x = \frac{1321}{711},\ y = \frac{1285}{711},\ z = \frac{1288}{711}.$$

His method is still interesting to peruse. He also wanted the minimum of $\{x, y, z\}$ to be $\sqrt{3}$, which he achieved.

In 1797/8, Legendre proved that the only positive integers n which are *not sums of three squares* are those of the form

$$n = 4^a(8b + 7), \text{ with } a, b > 0.$$

By contrast, one knows by Lagrange that *every positive integer is a sum of four squares.*

6. $X^4 + Y^4 = Z^2$ and Fermat

Fermat proved that this equation, and hence $X^4 + Y^4 = Z^4$, has no positive integral solutions, and in the process introduced the *Method of infinite descent.*

His argument: By the previous section, any solution (x, y, z) will need to satisfy $x^2 = 2mn$, $y^2 = m^2 - n^2$, implying that m or n is even, say m; then $y^2 + n^2$ is 0 modulo 4, forcing n to be even as well, leading to a smaller solution. One can continue this ad infinitum, resulting in a contradiction.

This case led Fermat to claim (in the 1630's) that $X^N + Y^N = Z^N$ has no positive integral solutions for $N \geq 3$. He claimed that the margin was too small to contain

his reasoning, but there seems to be a general scepticism that he had a proof. For $n = 3$, substantial progress was made a century late by Euler.

It is now elementary to observe that to establish FLT, it suffices to settle it for odd prime exponents.

7. Sophie Germain

Given that this lecture is in honor of Maryam Mirzakhani, it is imperative to point out a terrific female mathematician who made significant progress on the Fermat problem. Sophie Germain, born in 1776 in Paris, was extremely talented in Math, and since at that time the Ecole Polytechnique would not admit women, she could not attend the lectures of Lagrange there, but still followed them by getting the notes under a male psuedonym!

In the early eighteen hundreds she made a real breakthrough and proved the following:
Let p be any prime such that $2p+1$ is also a prime. Then there is no solution $(x, y.z)$ in whole numbers with $p \nmid xyz$ satisfying the Fermat equation $X^p + Y^p = Z^p$.

These primes are now called *Sophie Germain primes*, with obvious examples being $p = 5$ and $p = 11$. It is expected that there are infinitely many such primes, but this is still open.

8. Faltings

In 1983 the German mathematician Gerd Faltings supplied a dramatic proof (in [F]) of a *Conjecture of Mordell*, implying:

There are only a finite number of rational solutions (up to scaling) of the Fermat Equation $F_N : X^N + Y^N = Z^N$ for all $N \geq 4$.

In fact he proved this for solutions in any *number field*, i.e., a finite extension field K of $\mathbb{Q}$, and moreover, one could replace F_N by any plane curve defined by an irreducible polynomial equation of degree $> \sqrt{3}$ (so that each square is greater than 3, but they all add up to 10, making each square roughly of the same size).

This also showed the stark contrast between the number of (projective, meaning up to scaling) rational solutions of F_N for $N \leq 2$ and $N \geq 4$. One sees a *dichotomy* here. But in fact, there is a *trichotomy*.

9. View from Riemann Surfaces

Given a homogeneous polynomial $f(X, Y, Z)$, one always has the trivial (zero) solution, and any multiple of a given solution is another.

So one scales the solutions, to get an algebraic curve C defined by f in the *Projective plane* $\mathbb{P}^2$, which can be thought either as the space of lines through the origin in the (affine) three space, or as the compactification of the (affine) plane by adding a line at infinity.

When C is smooth, its complex solutions form a compact Riemann surface M, which has a genus g. (Simply speaking, a Riemann surface is a real surface on which one can measure angles.) Note that M is a *real surface* and a *complex curve*! (It of course makes sense as $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$.)

One can think of g as the number of handles one can attach to the Riemann sphere to obtain M (up to homeomorphism) or as the number of independent holomorphic differential 1-forms ω on M.

When M is defined by a homogeneous equation $f(X, Y, Z)$ of degree n, then g is given by $(n-1)(n-2)/2$. In particular the genus is > 1 when $N \geq 4$ and is 0 when $N \geq 2$.

What Mordell conjectured was that when $g \geq 2$, the number of rational points of C, embedded in M, is finite. This is what Faltings proved in its full generality!

10. The Trichotomy

In genus zero, as soon as one has a rational point, then there are infinitely many, in fact in bijection with the points on a projective line.

For example, the projective curve $X^2 + Y^2 + Z^2 = 0$ has no rational point at all, while F_2 defined by $X^2 + Y^2 - Z^2 = 0$ has infinitely many points.

And by Mordell (proved by Faltings), the number of rational points is finite for $g \geq 2$.

The case $g = 1$ is special; it has either no rational point, or else it is an *elliptic curve*, whose $\mathbb{Q}$-points form an abelian group $E(\mathbb{Q})$, known by Mordell to be isomorphic to $\mathbb{Z}^r \times G$, for a *finite group* G and r a non-negative integer, called the rank.

So in this intermediate (boundary) case, the number of points could in general be finite or infinite! For F_3, it happens to be finite.

11. Wiles and FLT

One would be remiss to not mention the deep and successful program of *Andrew Wiles*, completed in 1995, resulting in the establishment (in [W]) of **FLT for all** $N > 2$, partly relying on an important joint work with Richard Taylor ([TW]).

The proof is ingenious, involving a series of difficult arguments, but quite complicated for us to attempt to describe it here! It also involves deep results on elliptic curves and modular forms, and proceeds by establishing a modularity conjecture for elliptic curves over $\mathbb{Q}$, the sufficiency of which had earlier been established by K. Ribet using some ideas of G. Frey. The starting point of the strategy is to make use of the theorem of Langlands and Tunnell (cf. [La], [Tu]) that Artin's conjecture holds for Galois representations with image in $\mathrm{GL}_2(\mathbb{F}_3)$ (which is solvable), resulting in the modularity modulo 3 of any E.

For a thousand-word exposition, see https://simonsingh.net/books/fermats-last-theorem/the-whole-story/

In a related vein, a deep conjecture of J.-P. Serre asserting the modularity conjecture for odd 2-dimensional Galois representations was settled in 2005/8 by the elegant works of C. Khare and J.-P. Wintenberger [KW].

12. *L*-functions

To be concrete, let us look at elliptic curves E over $\mathbb{Q}$, defined by $Y^2 = f(X)$, with f a cubic polynomial with $\mathbb{Q}$-coefficients and distinct roots (in $\mathbb{C}$); For FLT, one

is interested in E such that f has three distinct roots in $\mathbb{Z}$. One can look at the number of points ν_p of the reduction of E modulo p, which will be non-singular at all p not dividing its conductor N. One sets $a_p = p + 1 - \nu_p$ for each p, and defines the L-function by the infinite (Euler) product

$$L(s, E) = \prod_p \frac{1}{1 - a_p p^{-s} + \omega(p) p^{1-2s}}$$

with $\omega(p) = 1$ iff $p \nmid N$ and $= 0$ otherwise. By a basic result of Hasse, one knows that $|a_p| \leq 2\sqrt{p}$, and this implies the normal convergence of $L(s, E)$ in $\Re(s) > 2$. The modularity of E signifies the existence of a (normalized new) cusp form f of weight 2, level N , with $\mathbb{Q}$-coefficients and trivial character, such that for each $p \nmid N$, a_p is the p-th Hecke eigenvalue of f. In other terms, the L-functions of E and f coincide (where an argument is needed at the bad P).

The utility of modularity for arithmetic is that by Hecke theory one knows that $L(s, f)$ admits a holomorphic continuation to the whole s-plane, and satisfies a functional equation relating s to $2 - s$, making $s = 11$ the critical center.

The modularity of arbitrary, not just semistable, elliptic curves over Q was accomplished (extending [TW], [W]), by the works of Brueil, Conrad, Diamond and Taylor (cf. [BCDT]).

For general V over $\mathbb{Q}$, the Langlands philosophy predicts a modularity, for each degree $j \geq 0$, of the degree j L-function $L^{(j)}(s, V)$ of the j-th cohomology $H^j(V)$ in terms of automorphic forms on $\mathrm{GL}(b_j)$ which are Hecke eigenforms (generating automorphic representations), where b_j is the j-th Betti number ($= \dim(H^j(V))$. (When V is an elliptic curve E, $L^{(1)}(s, E)$ is the L-function defined above, while $L^{(0)}(s, E) = \zeta(s)$ and $L^{(2)}(s, E) = \zeta(s-1)$, where $\zeta(s)$ is the Riemann Zeta function defined by the Dirichlet series $\sum_{n \geq 1} n^{-s}$ (in $\Re(s) > 1$). Some positive, striking results are known beyond elliptic curves, mostly tied up with modular (or Shimura) varieties ([Pic], [SSA]). Moreover, a fundmental new viewpoint has been brought to the subject by P. Scholze; see his recent works with A. Caraiani and others on the arxiv.

13. BSD

Let E be an elliptic curve over $\mathbb{Q}$. Then as noted earlier, one knows by Mordell that the (commutative) group $E(\mathbb{Q})$ of $\mathbb{Q}$-rational points on E is finitely generated, i.e., of the form $\mathbb{Z}^r \times H$, with H a finite group. The exponent r is the *rank* of $E(\mathbb{Q})$. It turns out, by a major theorem of Mazur that there are only a finite number of possibilities for H as one varies E over all elliptic curves over $\mathbb{Q}$; see [B1].

So the remaining (very) difficult problem is to understand the rank r. The famous *Conjecture of Birch and Swinnerton-Dyer*, colloquially referred to as BSD, predicts that r equals the order of zero at $s = 1$ of $L(s, E)$.

This is one of the Clay Millennial problems; see

https://www.claymath.org/millennium-problems/birch-and-swinnerton-dyer-conjecture

In particular, BSD predicts that when r is positive $L(s, E)$ must vanish. Here is the heuristic argument in that case: Suppose we ignore that fact that the Euler product expansion of $L(s, E)$ does not make sense at $s = 1$, and formally plug in

$s = 1$, we see that

$$L(1, E) \text{ “} ='' \prod_p \frac{p}{p - a_p + \omega(p)} = C \prod_{p \nmid N} \frac{p}{\nu_p}$$

with $C \neq 0$, where we have used $a_p = p + 1 - \nu_p$. When $r > 0$, one expects a lot of points mod p for lots of primes p, which by the Hasse bound implies that ν_p is close to $p + 1 + 2\sqrt{p}$ for many p, which results in the infinite product being zero, suggesting the same for $L(1, E)$.

There is an enormous body of literature on this fundamental conjecture with several partial, but striking, theorems. We will content ourselves to describing one recent result of Bhargava, Skinner and Wei Zhang [BSZ].

In this paper the authors show that over 60 percent of elliptic curves E over $\mathbb{Q}$, when ordered by the height, have $r = \text{ord}_{s=1} L(s, E) \leq 1$. Their method is to analyze the Selmer group at $p = 5$. If that can be done at an arbitrary p, then they can reach 100 percent (statistically).

14. Sato-Tate

Given any elliptic curve E over $\mathbb{Q}$, we may, thanks to the Hasse bound, write $a_p = 2\sqrt{p} \cos \theta_p$, for a phase $\theta_p \in [0, \pi] \subset \mathbb{R}$. When E admits complex multiplication (by an imaginary quadratic number), the distribution of the angles θ_p has been understood for some time.

In the non-CM case, an elegant conjecture of Sato and Tate, independently made, asserts that the angles θ_p are equidistributed on $[0, \pi]$ according to the measure $\frac{2}{\pi} \sin^2 \theta d\theta$. This conjecture was brilliantly solved by L. Clozel, M. Harris, N. Shepherd-Barron and R. Taylor (under a multiplicative reduction condition at a prime p) in an elaborate joint program, with the proof stretched over a series of three papers [CHT], [HST], [T].

Roughly speaking, these authors vastly generalize [TW] in the higher dimensional case, utilizing unitary Shimura varieties, and deduce the requisite analytic properties of $L(s, E, \text{sym}^n)$,the symmetric power L-functions of E.

A generalization valid for non-CM holomorphic newforms f of weight $k \geq 2$, removing also the multiplicative reduction condition for E attached to f of weight 2, was established in [BGHT].

A beautiful recent preprint of J. Newton and J.A. Thorne has made a breakthrough and established the modularity of all the symmetric powers of all semistable elliptic curves $E/\mathbb{Q}$, and of all newforms f of level 1 (cf. [NT]).

15. Hyperbolicity and Lang's Conjecture

The *Uniformization theorem* implies that every compact Riemann surface M of genus $g \geq 2$ is covered by the *upper half plane* $\mathcal{H} := \{x + iy \in \mathbb{C} \,|\, y > 0\}$, or equivalently the open unit disk in $\mathbb{C}$.

For $g = 0$ (resp. $g = 1$, the universal cover is the sphere S^2 (resp. the complex plane $\mathbb{C}$)

The natural Poincaré metric $dxdy/y^2$ on $\mathcal{H}$ furnishes a hyperbolic structure to M of genus ≥ 2, i.e., gives it *negative sectional curvature*. Note that for $g = 0$, (resp. $g = 1$), the curvature is positive (resp. 0).

Suppose V is a smooth projective variety of dimension n defined by a system of diophantine equations.

Let us call V *hyperbolic* if there is a non-constant holomorphic map $\varphi : \mathbb{C} \to M$, where M is the complex manifold (of complex dimension N) defined by the complex points of V.

Note that in dimension one, being hyperbolic is the same as the genus being ≥ 2.

Conjecture (Lang) *When V is hyperbolic, it is* **Mordellic**, *i.e., has only a finite number rational points, and in fact over any number field.*

This was partly inspired by groundbreaking work of Paul Vojta ([V]), who, through his analogy between Nevanlinna theory and Diophantine approximation, made his own strong conjectures.

For an insightful discussion of general conjectures on rational points, see [M2].

16. The Bombieri-Lang Conjecture

An algebro-geometric generalization of algebraic curves of genus $g \geq 2$ is given by the algebraic varieties of general type.

The Bombieri-Lang Conjecture asserts that for n-dimensional V of general type, the Zariski closure Z of the rational points has irreducible components of dimension $< n$.

When $n = 2$, i.e., when V is a surface, this conjecture is closely related to Lang's conjecture above. Indeed, for V a surface of general type, the *Bombieri-Lang Conjecture*asserts that the irreducible components of Z are all of dimension ≤ 1. If C is (the normalization of) a dimension one component, then C must have genus ≥ 2 if V is hyperbolic, as any C of genus ≤ 1 will have universal cover S^2 or $\mathbb{C}$, inducing a non-zero holomorphic map from $\mathbb{C}$ to $\mathcal{B}$, which is impossible. Then by Faltings, Z could have only a finite number of rational points, thereby yielding Mordellicity.

A very interesting situation is when $V = Y \cup D$ with Y open and hyperbolic, with D a divisor with normal crossings. Such a situation arises for the celebrated surfaces of Picard.

17. Picard Modular surfaces

Now we will focus on dimension 2, i.e., when V is a smooth projective surface which is itself hyperbolic or contains an open surface Y which is hyperbolic.

Here, hyperbolicity does not guarantee the universal cover being the unit disk $\mathcal{B}$ in $\mathbb{C}^2$.

However, many beautiful examples are furnished by the *Picard modular surfaces* $Y(\mathbb{C}) = \Gamma\backslash\mathcal{B}$, which have smooth compactifications $V(\mathbb{C})$ with complement a divisor D with normal crossings.

Γ is a discrete subgroup of finite covolume in $SU(2,1)$ defined by a hermitian form on K^3 with K an imaginary quadratic field. It is known that such quotients admit models over number fields.

The divisor D at infinity turns out to be a finite union of elliptic curves with complex multiplication by K.

Much is known about these surfaces - due to J. Rogawski, R. Kottwitz, J.S. Milne and others [Pic], [Ro].

Here is something this lecturer proved jointly with Mladen Dimitrov [DR].

Theorem *Let $V = Y \cup D$ be a Picard modular surface as above relative to an arithmetic subgroup Γ of $SU(2,1)$. Then Lang's conjecture holds for a finite cover Y' of Y.*

As a consequence, one gets Mordellicity of surfaces Y which arise this way.

There is also a version establishing an analogue for compact arithmetic quotients X of $\mathcal{B}$. In that case, the result had earlier been known (by a different method) by Emmanuel Ullmo.

One gets examples this way of general type surfaces arising as intersections of hypersurfaces in $\mathbb{P}^n$. A particularly simple one is the surface in $\mathbb{P}^5$ given by the solution set of the Diophantine system of equations:

$$x_1^5 + y^5 = z^5,\ x_2^5 + z^5 = w^5,\ x_3^5 + w^5 = y^5,$$

which involves the familiar Fermat equations.

If a beginner wants more information on the rudiments of Number theory, zie could look at the author's Notes: *Introduction to Number Theory* at http://www.its.caltech.edu/ dinakar/

References

[BGHT] T. Barnet-Lamb, D. Geraghty, M. Harris, Michael and R. Taylor, A family of Calabi-Yau varieties and potential automorphy II, Publ. Res. Inst. Math. Sci. 47 (2011), no. 1, 29—98.

[BSZ] M. Bhargava, C. Skinner and Wei Zhang, *A majority of elliptic curves over Q satisfy the Birch and Swinnerton-Dyer conjecture*, (2014). https://arxiv.org/abs/1407.1826v2

[BCDT] C. Breuil, B. Conrad, Brian, F. Diamond and R. Taylor, On the modularity of elliptic curves over Q: wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001), no. 4, 843—939.

[CHT] L. Clozel, M. Harris and R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations, with Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras, Publ. Math. Inst. Hautes Études Sci. No. 108 (2008), 1—181.

[DR] M. Dimitrov and D. Ramakrishnan, Arithmetic quotients of the complex ball and a conjecture of Lang. (English summary) Doc. Math. 20 (2015), 1185–1205.

[D] Diophantus, *Arithmetica* (Greek); Latin translation by Claude Gaspard Bachet de Méziriac; English translation by Sir Thomas L. Heath (1910): archive.org/details/diophantusofalex00heatiala

[F] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* (German) [Finiteness theorems for abelian varieties over number fields] Invent. Math. 73 (1983), no. 3, 349—366.

[HST] M. Harris, N. Shepherd-Barron and R. Taylor, A family of Calabi-Yau varieties and potential automorphy, Ann. of Math. (2) 171 (2010), no. 2, 779—813.

[KW] C. Khare and J.-L. Wintenberger, Serre's modularity conjecture. Proceedings of the International Congress of Mathematicians. Volume II, 280—293, Hindustan Book Agency, New Delhi, 2010.

[La] R.P. Langlands, *Base change for GL(2)*, Annals of Mathematics Studies **96**. Princeton University Press (1980).

[B1] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. 44 (1978), no. 2, 129—162.

[M2] B. Mazur, *Open problems regarding rational points on curves and varieties*, Galois representations in arithmetic algebraic geometry (Durham, 1996), 239–265, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[NT] J. Newton and J.A. Thorne, Symmetric Power Functoriality For Holomorphic Modular Forms, arXiv:1912.11261v1 [math.NT] 24 Dec 2019.

[Pic] *T*he zeta functions of Picard modular surfaces, edited by R.P. Langlands and D. Ramakrishnan, CRM Publications, Univ. Montréal, Montreal, QC (1992).

[Ro] J. Rogawski, *A*utomorphic representations of unitary groups in three variables, Annals of Mathematics Studies, **123**, Princeton University Press, Princeton, NJ, 1990.

[Sch] N. Schappacher, "Wer war Diophant?" (German) ["Who was Diophantus?"] Math. Semesterber. 45 (1998), no. 2, 141—156 (English translation: http://irma.math.unistra.fr/ schappa/NSch/Publications files/1998cBis Dioph.pdf)

[SSA] *S*tabilization of the Trace Formula, Shimura Varieties, and Arithmetic Applications, edited by L. Clozel, M. Harris, J.-P. Labesse and B.-C. Ngo, Books 1,2, International Press, Sommerville, MA (2011).

[T] R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations II, Publ. Math. Inst. Hautes Études Sci. No. 108 (2008), 183—239.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141 (1995), no. 3, 553-–572.

[Tu] J. Tunnell, Artin's conjecture for representations of octahedral type. Bull. Amer. Math. Soc. (N.S.) 5 (1981), no. 2, 173—175.

[V] P. Vojta, Nevanlinna theory and Diophantine approximation. Several complex variables (Berkeley, CA, 1995–1996), 535–564, Math. Sci. Res. Inst. Publ., 37, Cambridge Univ. Press, Cambridge, 1999.

[W] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (1995), no. 3, 443—551.

[We] A. Weil, *Number theory. An approach through history from Hammurapi to Legendre*, Reprint of the 1984 edition. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA (2007).