Glimpses of Algebra and Geometry, Second Edition

Gabor Toth

Springer

Undergraduate Texts in Mathematics

Readings in Mathematics

Editors

S. Axler
F.W. Gehring
K.A. Ribet

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Gabor Toth

Glimpses of Algebra and Geometry

Second Edition

With 183 Illustrations, Including 18 in Full Color

Springer

Gabor Toth
Department of Mathematical Sciences
Rutgers University
Camden, NJ 08102
USA
gtoth@camden.rutgers.edu

Front cover illustration: The regular compound of five tetrahedra given by the face-planes of a colored icosahedron. The circumscribed dodecahedron is also shown. Computer graphic made by the author using Geomview. *Back cover illustration*: The regular compound of five cubes inscribed in a dodecahedron. Computer graphic made by the author using *Mathematica*®.

Mathematics Subject Classification (2000): 15-01, 11-01, 51-01

Library of Congress Cataloging-in-Publication Data
Toth, Gabor, Ph.D.
Glimpses of algebra and geometry/Gabor Toth.—2nd ed.
p. cm. — (Undergraduate texts in mathematics. Readings in mathematics.)
Includes bibliographical references and index.
ISBN 0-387-95345-0 (hardcover: alk. paper)
1. Algebra. 2. Geometry. I. Title. II. Series.
QA154.3 .T68 2002
512′.12—dc21 2001049269

Printed on acid-free paper.

Production managed by Francine McNeill; manufacturing supervised by Jeffrey Taub.
Typeset from the author's LaTeX2e files using Springer's UTM style macro by The Bartlett Press, Inc., Marietta, GA.
Printed and bound by Hamilton Printing Co., Rensselaer, NY.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-95345-0 SPIN 10848701

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

This book is dedicated to my students.

Preface to the Second Edition

Since the publication of the Glimpses in 1998, I spent a considerable amount of time collecting "mathematical pearls" suitable to add to the original text. As my collection grew, it became clear that a major revision in a second edition needed to be considered. In addition, many readers of the Glimpses suggested changes, clarifications, and, above all, more examples and worked-out problems. This second edition, made possible by the ever-patient staff of Springer-Verlag New York, Inc., is the result of these efforts. Although the general plan of the book is unchanged, the abundance of topics rich in subtle connections between algebra and geometry compelled me to extend the text of the first edition considerably. Throughout the revision, I tried to do my best to avoid the inclusion of topics that involve very difficult ideas.

The major changes in the second edition are as follows:

1. An in-depth treatment of root formulas solving quadratic, cubic, and quartic equations à la van der Waerden has been given in a new section. This can be read independently or as preparation for the more advanced new material encountered toward the later parts of the text. In addition to the Bridge card symbols, the dagger † has been introduced to indicate more technical material than the average text.

2. As a natural continuation of the section on the Platonic solids, a detailed and complete classification of finite Möbius groups à la Klein has been given with the necessary background material, such as Cayley's theorem and the Riemann–Hurwitz relation.
3. One of the most spectacular developments in algebra and geometry during the late nineteenth century was Felix Klein's theory of the icosahedron and his solution of the irreducible quintic in terms of hypergeometric functions. A quick, direct, and modern approach of Klein's main result, the so-called *Normalformsatz*, has been given in a single large section. This treatment is independent of the material in the rest of the book, and is suitable for enrichment and undergraduate/graduate research projects. All known approaches to the solution of the irreducible quintic are technical; I have chosen a geometric approach based on the construction of canonical quintic resolvents of the equation of the icosahedron, since it meshes well with the treatment of the Platonic solids given in the earlier part of the text. An algebraic approach based on the reduction of the equation of the icosahedron to the Brioschi quintic by Tschirnhaus transformations is well documented in other textbooks. Another section on polynomial invariants of finite Möbius groups, and two new appendices, containing preparatory material on the hypergeometric differential equation and Galois theory, facilitate the understanding of this advanced material.
4. The text has been upgraded in many places; for example, there is more material on the congruent number problem, the stereographic projection, the Weierstrass $\wp$-function, projective spaces, and isometries in space.
5. The new Web site at http://mathsgi01.rutgers.edu/~gtoth/Glimpses/ containing various text files (in PostScript and HTML formats) and over 70 pictures in full color (in gif format) has been created.
6. The historical background at many places of the text has been made more detailed (such as the ancient Greek approximations of π), and the historical references have been made more precise.
7. An extended solutions manual has been created containing the solutions of 100 problems.

I would like to thank the many readers who suggested improvements to the text of the first edition. These changes have all been incorporated into this second edition. I am especially indebted to Hillel Gauchman and Martin Karel, good friends and colleagues, who suggested many worthwhile changes. I would also like to express my gratitude to Yukihiro Kanie for his careful reading of the text and for his excellent translation of the first edition of the Glimpses into Japanese, published in early 2000 by Springer-Verlag, Tokyo. I am also indebted to April De Vera, who upgraded the list of Web sites in the first edition. Finally, I would like to thank Ina Lindemann, Executive Editor, Mathematics, at Springer-Verlag New York, Inc., for her enthusiasm and encouragement throughout the entire project, and for her support for this early second edition.

Camden, New Jersey Gabor Toth

Preface to the First Edition

Glimpse: 1. a very brief passing look, sight or view. 2. a momentary or slight appearance. 3. a vague idea or inkling.

—*Random House College Dictionary*

At the beginning of fall 1995, during a conversation with my respected friend and colleague Howard Jacobowitz in the Octagon Dining Room (Rutgers University, Camden Campus), the idea emerged of a "bridge course" that would facilitate the transition between undergraduate and graduate studies. It was clear that a course like this could not concentrate on a single topic, but should browse through a number of mathematical disciplines. The selection of topics for the Glimpses thus proved to be of utmost importance. At this level, the most prominent interplay is manifested in some easily explainable, but eventually subtle, connections between number theory, classical geometries, and modern algebra. The rich, fascinating, and sometimes puzzling interactions of these mathematical disciplines are seldom contained in a medium-size undergraduate textbook. The Glimpses that follow make a humble effort to fill this gap.

The connections among the disciplines occur at various levels in the text. They are sometimes the main topics, such as Rationality and Elliptic Curves (Section 3), and are sometimes hidden in problems, such as the spherical geometric proof of diagonalization of Euclidean isometries (Problems 1 to 2, Section 16), or the proof of Euler's theorem on convex polyhedra using linear algebra (Problem 9, Section 20). Despite numerous opportunities throughout the text, the experienced reader will no doubt notice that analysis had to be left out or reduced to a minimum. In fact, a major source of difficulties in the intense 8-week period during which I produced the first version of the text was the continuous cutting down of the size of sections and the shortening of arguments. Furthermore, when one is comparing geometric and algebraic proofs, the geometric argument, though often more lengthy, is almost always more revealing and thereby preferable. To strive for some originality, I occasionally supplied proofs out of the ordinary, even at the "expense" of going into calculus a bit. To me, "bridge course" also meant trying to shed light on some of the links between the first recorded intellectual attempts to solve ancient problems of number theory, geometry, and twentieth-century mathematics. Ignoring detours and sidetracks, the careful reader will see the continuity of the lines of arguments, some of which have a time span of 3000 years. In keeping this continuity, I eventually decided not to break up the Glimpses into chapters as one usually does with a text of this size. The text is, nevertheless, broken up into subtexts corresponding to various levels of knowledge the reader possesses. I have chosen the card symbols ♣, ♢, ♡, ♠ of Bridge to indicate four levels that roughly correspond to the following:

♣ College Algebra;
♢ Calculus, Linear Algebra;
♡ Number Theory, Modern Algebra (elementary level), Geometry;
♠ Modern Algebra (advanced level), Topology, Complex Variables.

Although much of ♡ and ♠ can be skipped at first reading, I encourage the reader to challenge him/herself to venture occasionally into these territories. The book is intended for (1) students (♣ and ♢) who wish to learn that mathematics is more than a set of tools (the way sometimes calculus is taught), (2) students (♡ and ♠) who

love mathematics, and (3) high-school teachers ($\subset \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$) who always had keen interest in mathematics but seldom time to pursue the technicalities.

Reading what I have written so far, I realize that I have to make one point clear: Skipping and reducing the size of subtle arguments have the inherent danger of putting more weight on intuition at the expense of precision. I have spent a considerable amount of time polishing intuitive arguments to the extent that the more experienced reader can make them withstand the ultimate test of mathematical rigor.

Speaking (or rather writing) of danger, another haunted me for the duration of writing the text. One of my favorite authors, Iris Murdoch, writes about this in *The Book and the Brotherhood*, in which Gerard Hernshaw is badgered by his formidable scholar Levquist about whether he wanted to write mediocre books out of great ones for the rest of his life. (To learn what Gerard's answer was, you need to read the novel.) Indeed, a number of textbooks influenced me when writing the text. Here is a sample:

1. M. Artin, *Algebra*, Prentice-Hall, 1991;
2. A. Beardon, *The Geometry of Discrete Groups*, Springer-Verlag, 1983;
3. M. Berger, *Geometry I–II*, Springer-Verlag, 1980;
4. H.S.M. Coxeter, *Introduction to Geometry*, Wiley, 1969;
5. H.S.M. Coxeter, *Regular Polytopes*, Pitman, 1947;
6. D. Hilbert and S. Cohn-Vossen, *Geometry and Imagination*, Chelsea, 1952.
7. J. Milnor, *Topology from the Differentiable Viewpoint*, The University Press of Virginia, 1990;
8. I. Niven, H. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, Wiley, 1991;
9. J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

Although I (unavoidably) use a number of by now classical arguments from these, originality was one of my primary aims. This book was never intended for comparison; my hope is that the Glimpses may trigger enough motivation to tackle these more advanced textbooks.

Despite the intertwining nature of the text, the Glimpses contain enough material for a variety of courses. For example, a shorter version can be created by taking Sections 1 to 10 and Sections 17 and 19 to 23, with additional material from Sections 15 to 16 (treating Fuchsian groups and Riemann surfaces marginally via the examples) when needed. A nonaxiomatic treatment of an undergraduate course on geometry is contained in Sections 5 to 7, Sections 9 to 13, and Section 17.

The Glimpses contain a lot of computer graphics. The material can be taught in the traditional way using slides, or interactively in a computer lab or teaching facility equipped with a PC or a workstation connected to an LCD-panel. Alternatively, one can create a graphic library for the illustrations and make it accessible to the students. Since I have no preference for any software packages (although some of them are better than others for *particular* purposes), I used both *Maple*®[1] and *Mathematica*®[2] to create the illustrations. In a classroom setting, the link of either of these to Geomview[3] is especially useful, since it allows one to manipulate three-dimensional graphic objects. Section 17 is highly graphic, and I recommend showing the students a variety of slides or three-dimensional computer-generated images. Animated graphics can also be used, in particular, for the action of the stereographic projection in Section 7, for the symmetry group of the pyramid and the prism in Section 17, and for the cutting-and-pasting technique in Sections 16 and 19. These Maple® text files are downloadable from my Web sites

http://carp.rutgers.edu/math-undergrad/science-vision.html
and
http://mathsgi01.rutgers.edu/~gtoth/.

Alternatively, to obtain a copy, write an e-mail message to

gtoth@camden.rutgers.edu

[1] Maple is a registered trademark of Waterloo Maple, Inc.

[2] *Mathematica* is a registered trademark of Wolfram Research, Inc.

[3] A software package downloadable from the Web site: http://www.geom.umn.edu.

or send a formatted disk to Gabor Toth, Department of Mathematical Sciences, Rutgers University, Camden, NJ 08102, USA.

A great deal of information, interactive graphics, animations, etc., are available on the World Wide Web. I highly recommend scheduling at least one visit to a computer or workstation lab and explaining to the students how to use the Web. In fact, at the first implementation of the Glimpses at Rutgers, I noticed that my students started spending more and more time at various Web sites related to the text. For this reason, I have included a list of recommended Web sites and films at the end of some sections. Although hundreds of Web sites are created, upgraded, and terminated daily, every effort has been made to list the latest Web sites currently available through the Interent.

Camden, New Jersey Gabor Toth

Acknowledgments

The second half of Section 20 on the four color theorem was written by Joseph Gerver, a colleague at Rutgers. I am greatly indebted to him for his contribution and for sharing his insight into graph theory. The first trial run of the Glimpses at Rutgers was during the first six weeks of summer 1996, with an equal number of undergraduate and graduate students in the audience. In fall 1996, I also taught undergraduate geometry from the Glimpses, covering Sections 1 to 10 and Sections 17 and 19 to 23. As a result of the students' dedicated work, the original manuscript has been revised and corrected, some of the arguments have been polished, and some extra topics have been added. It is my pleasure to thank all of them for their participation, enthusiasm, and hard work. I am particularly indebted to Jack Fistori, a mathematics education senior at Rutgers, who carefully revised the final version of the manuscript, making numerous worthwhile changes. I am also indebted to Susan Carter, a graduate student at Rutgers, who spent innumerable hours at the workstation to locate suitable Web sites related to the Glimpses. In summer 1996, I visited the Geometry Center at the University of Minnesota. I lectured about the Glimpses to an audience consisting of undergraduate and graduate students and high-school teachers. I wish to thank them for their valuable comments, which I took

into account in the final version of the manuscript. I am especially indebted to Harvey Keynes, Education Director of the Geometry Center, for his enthusiastic support of the Glimpses. During my stay, I produced a 10-minute film *Glimpses of the Five Platonic Solids* with Stuart Levy, whose dedication to the project surpassed all my expectations. The typesetting of the manuscript started when I gave the first 20 pages to Betty Zubert as material with which to practice LaTeX. As the manuscript grew beyond any reasonable size, it is my pleasure to record my thanks to her for providing inexhaustible energy that turned 300 pages of chicken scratch into a fine document.

Camden, New Jersey Gabor Toth

Contents

SECTION 1 "A Number Is a Multitude Composed of Units"—Euclid

♣ We adopt Kronecker's phrase: "God created the natural numbers, and all the rest is the work of man," and start with the set

$$\mathbf{N} = \{1, 2, 3, 4, 5, 6, \ldots\}$$

of all *natural numbers*. Since the sum of two natural numbers is again a natural number, $\mathbf{N}$ carries the operation[1] of addition $+ : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$.

Remark.
Depicting natural numbers by arabic numerals is purely traditional. Romans might prefer

$$\mathbf{N} = \{\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}, \mathrm{V}, \mathrm{VI}, \ldots\},$$

and computers work with

$$\mathbf{N} = \{1, 10, 11, 100, 101, 110, \ldots\}.$$

Notice that converting a notation into another is nothing but an *isomorphism* between the respective systems. Isomorphism respects

[1] If needed, please review "Sets" and "Groups" in Appendices A and B.

addition; for example, $29+33 = 62$ is the same as XXIX + XXXIII = LXII or $11101 + 100001 = 111110$.

From the point of view of group theory, $\mathbf{N}$ is a failure; it does not have an identity element (that we would like to call zero) and no element has an inverse. We remedy this by extending $\mathbf{N}$ to the (additive) *group of integers*

$$\mathbf{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \ldots\}.$$

$\mathbf{Z}$ also carries the operation of multiplication $\times : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$. Since distributivity holds, $\mathbf{Z}$ forms a *ring* with respect to addition and multiplication.

Although we have 1 as the identity element with respect to $\times$, we have no hope for $\mathbf{Z}$ to be a multiplicative group; remember the saying: "Thou shalt not divide by zero!" To remedy this, we delete the ominous zero and consider

$$\mathbf{Z}^{\#} = \mathbf{Z} - \{0\} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \ldots\}.$$

The requirement that integers have inverses gives rise to fractions or, more appropriately, *rational numbers*:

$$\mathbf{Q} = \mathbf{Q}^{\#} \cup \{0\} = \{a/b \mid a, b \in \mathbf{Z}^{\#}\} \cup \{0\},$$

where we put the zero back to save the additive group structure. All that we learned in dealing with fractions can be rephrased elegantly by saying that $\mathbf{Q}$ is a *field*: $\mathbf{Q}$ is an additive group, $\mathbf{Q}^{\#}$ is an abelian (i.e., commutative) multiplicative group, and addition and multiplication are connected through distributivity.

After having created $\mathbf{Z}$ and $\mathbf{Q}$, the direction we take depends largely on what we wish to study. In elementary number theory, when studying divisibility properties of integers, we consider, for a given $n \in \mathbf{N}$, the (additive) group $\mathbf{Z}_n$ of *integers modulo* n. The simplest way to understand

$$\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z} = \{[0], [1], \ldots, [n-1]\}$$

is to start with $\mathbf{Z}$ and to *identify* two integers a and b if they differ by a multiple of n. This identification is indicated by the square bracket; $[a]$ means a plus all multiples of n. Clearly, no numbers are identified among $0, 1, \ldots, n-1$, and any integer is identified

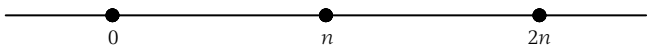

Figure 1.1

with exactly one of these. The (additive) group structure is given by the usual addition in $\mathbf{Z}$. More explicitly, $[a]+[b] = [a+b]$, $a, b \in \mathbf{Z}$. Clearly, $[0]$ is the zero element in $\mathbf{Z}_n$, and $-[a] = [-a]$ is the additive inverse of $[a] \in \mathbf{Z}_n$. Arithmetically, we use the division algorithm to find the quotient q and the remainder $0 \leq r < n$, when $a \in \mathbf{Z}$ is divided by n:

$$a = qn + r,$$

and set $[a] = [r]$. The geometry behind this equality is clear. Consider the multiples of n, $n\mathbf{Z} \subset \mathbf{Z}$, as a *one-dimensional lattice* (i.e., an infinite string of equidistantly spaced points) in $\mathbf{R}$ as in Figure 1.1. Now locate a and its closest left neighbor qn in $n\mathbf{Z}$ (Figure 1.2). The distance between qn and a is r, the latter between 0 and $n-1$. Since a and r are to be identified, the following geometric picture emerges for $\mathbf{Z}_n$: Wrap $\mathbf{Z}$ around a circle infinitely many times so that the points that overlap with 0 are exactly the lattice points in $n\mathbf{Z}$; this can be achieved easily by choosing the radius of the circle to be $n/2\pi$. Thus, $\mathbf{Z}_n$ can be visualized as n equidistant points on the perimeter of a circle (Figure 1.3). Setting the center of the circle at the origin of a coordinate system on the Cartesian plane $\mathbf{R}^2$ such that $[0]$ is the intersection point of the circle and the positive first axis, we see that addition in $\mathbf{Z}_n$ corresponds to *addition of angles of the corresponding vectors*. A common convention is to choose the positive orientation as the way $[0], [1], [2], \ldots$ increase. This picture of $\mathbf{Z}_n$ as the vertices of a *regular n-sided polygon* (with angular addition) will recur later on in several different contexts.

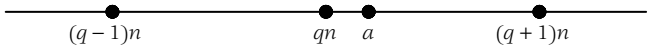

Figure 1.2

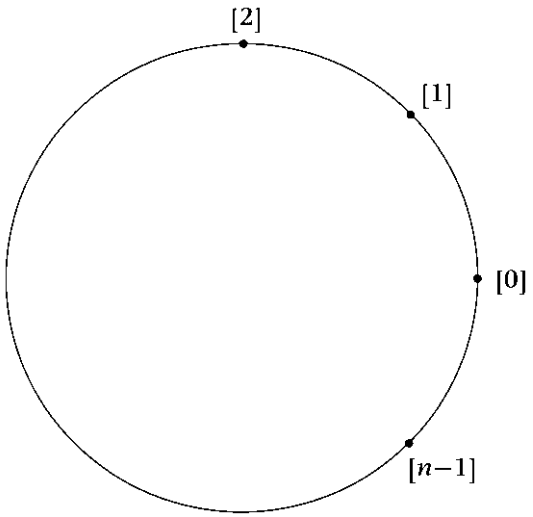

Figure 1.3

Remark.
In case you've ever wondered why it was so hard to learn the clock in childhood, consider $\mathbf{Z}_{60}$. Why the Babylonian choice[2] of 60? Consider natural numbers between 1 and 100 that have the largest possible number of small divisors.

♡ The infinite $\mathbf{Z}$ and its finite offsprings $\mathbf{Z}_n$, $n \in \mathbf{N}$, share the basic property that they are generated by a single element, a property that we express by saying that $\mathbf{Z}$ and $\mathbf{Z}_n$ are *cyclic*. In case of $\mathbf{Z}$, this element is 1 or -1; in case of $\mathbf{Z}_n$, a generator is $[1]$.

♣ You might be wondering whether it is a good idea to reconsider multiplication in $\mathbf{Z}_n$ induced from that of $\mathbf{Z}$. The answer is yes; multiplication in $\mathbf{Z}$ gives rise to a well-defined multiplication in $\mathbf{Z}_n$ by setting $[a] \cdot [b] = [ab]$, $a, b \in \mathbf{Z}$. Clearly, $[1]$ is the multiplicative identity element. Consider now multiplication restricted to $\mathbf{Z}_n^{\#} = \mathbf{Z}_n - \{[0]\}$. There is a serious problem here. If n is composite, that is, $n = ab$, $a, b \in \mathbf{N}$, $a, b \geq 2$, then $[a], [b] \in \mathbf{Z}_n^{\#}$, but $[a] \cdot [b] = [0]$! Thus, multiplication restricted to $\mathbf{Z}_n^{\#}$ is not even an operation.

[2]Actually, a number system using 60 as a base was developed by the Sumerians about 500 years before it was passed on to the Babylonians around 2000 B.C.

We now pin our hopes on $\mathbf{Z}_p$, where p a prime. Elementary number theory says that if p divides ab, then p divides either a or b. This directly translates into the fact that $\mathbf{Z}_p^{\#}$ is closed under multiplication. Encouraged by this, we now go a step further and claim that $\mathbf{Z}_p^{\#}$ is a multiplicative group! Since associativity follows from associativity of multiplication in $\mathbf{Z}$, it remains to show that each element $a \in \mathbf{Z}_p^{\#}$ has a multiplicative inverse. To prove this, multiply the complete list $[1], [2], \ldots, [p-1]$ by $[a]$ to obtain

$$[a], [2a], \ldots, [(p-1)a].$$

By the above, these all belong to $\mathbf{Z}_p^{\#}$. They are mutually disjoint. Indeed, assume that $[ka] = [la]$, $k, l = 1, 2, \ldots, p-1$. We then have $[(k-l)a] = [k-l] \cdot [a] = [0]$, so that $k = l$ follows. Thus, the list above gives $p-1$ elements of $\mathbf{Z}_p^{\#}$. But the latter consists of exactly $p-1$ elements, so we got them all! In particular, $[1]$ is somewhere in this list, say, $[\bar{a}a] = [1]$, $\bar{a} = 1, \ldots, p-1$. Hence, $[\bar{a}]$ is the multiplicative inverse of $[a]$. Finally, since distributivity in $\mathbf{Z}_p$ follows from distributivity in $\mathbf{Z}$, we obtain that $\mathbf{Z}_p$ is a field for p prime.

We give two applications of these ideas: one for $\mathbf{Z}_3$ and another for $\mathbf{Z}_4$. First, we claim that if 3 divides $a^2 + b^2$, $a, b \in \mathbf{Z}$, then 3 divides both a and b. Since divisibility means zero remainder, all we have to count is the sum of the remainders when a^2 and b^2 are divided by 3. In much the same way as we divided all integers to even $(2k)$ and odd $(2k+1)$ numbers $(k \in \mathbf{Z})$, we now write $a = 3k, 3k+1, 3k+2$ accordingly. Squaring, we obtain $a^2 = 9k^2, 9k^2 + 6k + 1, 9k^2 + 12k + 4$. Divided by 3, these give remainders 0 or 1, with 0 corresponding to a being a multiple of 3. The situation is the same for b^2. We see that when dividing $a^2 + b^2$ by 3, the possible remainders are $0+0, 0+1, 1+0, 1+1$, and the first corresponds to a and b both being multiples of 3. The first claim follows.

Second, we show the important number theoretical fact that no number of the form $4m + 3$ is a sum of two squares of integers. (Notice that, for $m = 0$, this follows from the first claim or by inspection.) This time we study the remainder when $a^2 + b^2$, $a, b \in \mathbf{Z}$, is divided by 4. Setting $a = 4k, 4k+1, 4k+2, 4k+3$, a^2 gives remainders 0 or 1. As before, the possible remainders for $a^2 + b^2$ are $0+0, 0+1, 1+0, 1+1$. The second claim also follows.