Confronting Euro-Centrism and Erasure In Discrete Math

Theodore Kim
Department of Computer Science
Yale University

January 2021

Abstract

This is a summary of measures I took in Fall 2020 to confront Euro-Centrism and the historical erasure of non-Western figures in a discrete math course, *CPSC 202: Mathematical Tools for Computer Science*. These measures included investigations of Boolean logic and Pascal's Triangle, and an examination of the naming double standards applied to Euclid's Algorithm vs. the Chinese Remainder Theorem. Students were given the opportunity to investigate the history further as an optional bonus assignment in the run-up to the 2020 US presidential election. I also summarize some of their remarkable findings.

1 Introduction

In the Fall of 2020, I taught the introductory discrete math course in Yale Computer Science, *CPSC 202: Mathematical Tools for Computer Science*. It touches on several non-discrete topics, but is mostly composed of discrete classics like Boolean logic, mathematical induction, sets, and the pigeonhole principle. It is the main course that introduces discrete math to computer science undergraduates at Yale.

This was my first time teaching this course, but I was already aware that when historical context is presented in discrete math courses, it usually traces ideas back to ancient Greece. However, preparations for this course took place in Summer 2020, in the midst of nationwide protests repudiating white supremacy and calling for racial justice in the wake of the murders of George Floyd, Ahmaud Arbery, Breonna Taylor, and many, many others. Against this background, I decided that it was important to expand the historical context of this course beyond the traditional Euro-centric lens of "pale and male."

The following are examples of non-Western history that I presented alongside the usual technical material. Student findings from a non-required assignment are summarized as well.

2 Boolean Logic

Boolean logic underlies vast swaths of computer science, and is named after George Boole (1815–1864) due to his groundbreaking works *The Mathematical Analysis of Logic* (1847) and *An Investigation of the Laws of Thought* (1854). We covered Boolean logic early on in the course, and also covered De Morgan's laws, which were established by his contemporary, Augustus De Morgan (1806–1871).

After presenting the basic mechanics of this logic, I asked an obvious contextualizing question: who were Boole's intellectual forebears, and how did they shape his thinking? Again, the traditional approach is to enumerate connections back to ancient Greece.

However, this approach was already being disputed in Boole's time by his most intimate of acquaintances: his mathematician wife, Mary Everest Boole (1832–1916). In her 1901 letter *Indian Thought and Western Science in the Nineteenth Century*, written 37 years after her husband's death, Mary Everest Boole laid out a more expansive picture of how George Boole was influenced by Hindu, by which she meant Indian[1], thought. She also detailed how her contemporaries actively suppressed these connections:

> *Scientific men, theologians and publishers alike, invited me to throw light on some passages in my husband's works which they felt obscure; but every attempt on my part to interpret "Boole's Equation" as a law of the human mind known in Asia from the earliest recorded ages met with either violent opposition or blank non-intelligence. My adventures among the learned would fill a volume, and very funny reading it would be, though in some parts very sad.*

In modern terms, Mary Everest Boole is describing *erasure*: the practice of rendering invisible the contributions of certain groups or individuals.

Mary Everest Boole's claim was that her uncle, Sir George Everest, for whom Mount Everest is named, brought Hindu mathematical ideas back from his extensive travels in India. He then communicated these ideas to his contemporaries, including Charles Babbage, Augustus De Morgan, and George Boole. She presented De Morgan's 1859 sponsorship of the London publication of *Treatise on Maxima and Minima* by the Indian mathematician Ram Chundra as evidence of his esteem for this school of thought, as well the ideas for singular points on curves in Babbage's *Ninth Bridgewater Treatise*, which closely matched notions from "Hindu metaphysic(s)."

Primary source evidence is also available, such as the following passage from De Morgan's *Syllabus of a Proposed System of Logic* (1860, Fig. 1):

> *The two races which have founded mathematics, those of the Sanskrit and Greek languages, have been the two which have independently formed systems of logic.*

While De Morgan otherwise hews to the Greek tradition, his awareness and regard of the Sanskrit (Indian) tradition in this passage is plainly visible.

The purpose of presenting these events was threefold. First, to underscore that non-white and non-Western people independently developed many of the ideas we normally attribute solely to the West, and in fact influenced the formulations in common use. Second, that these contributions were actively erased and suppressed. The "pale and male" tradition of today was deliberately shaped by past prejudices. This is not to accuse Boole or De Morgan of theft or appropriation (I found no evidence of this), but rather to affirm that the construction of modern math and the science has always been a global project. Finally, Mary Everest Boole was a woman, and consequently in a socially disadvantaged position during her lifetime. The fact that she still spoke out against the erasure of others from her already underprivileged position deserves recognition. In modern terms, she chose to be an *ally*.

Investigations into George Boole's influences from India continue into modern times, such as with Subhash Kak's 2018 article, *George Boole's "Laws of Thought" and Indian logic*. They paint a fascinating alternate mathematical tradition, where the motivation for discovering new theorems is (to use modern Judeo-Christian language) to bring yourself "closer to God." Our current boundary between science and religion stretches back to the Enlightenment, but it was not inevitable, and other worlds are possible where they commingle and mutually inspire.

[1]India is a nation, while Hinduism is a religion, so this correspondence encodes many colonial assumptions. These distinctions resonate even in modern-day Indian politics, and are far too complex to parse in a single footnote.

3 Pascal's Triangle

When covering "n choose k" notation, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, we also covered *Pascal's Triangle*, a triangle of numbers that naturally arises from this combinatoric mechanism. This topic presented an opportunity to explore how names come to be assigned to mathematical concepts.

Pascal's Triangle is named after Blaise Pascal (1623–1662), a well-known French mathematician who has a variety of concepts named after him. For example, the Pascal programming language was used to create the very first version of the Apple Macintosh operating system. That specific naming is honorary, while the term *Pascal's Triangle* implies that he first discovered the concept of the combinatoric triangle.

The purpose of presenting this example was to show that this implication is entirely false. The history of the triangle goes backwards in time for more than a millennium, and stretches across multiple cultures spanning the entire globe. Working backwards from the 17th century, the Italian Niccolo Tartaglia (1500–1577) also discovered the triangle. In Italy, it is still sometimes referred to as "Tartaglia's Triangle". The current primacy of Pascal speaks to the dominance of French mathematics in the 17th century. Meanwhile, the Chinese mathematicians Jia Xian (1010–1070) and Yang Hui (1238–1298) also have claim to the triangle, and in China it is still sometimes called "Yang Hui's Triangle."

Perhaps the most interesting claim is that of Omar Khayyam (1048–1131) from Persia (modern day Iran), where it is still sometimes called a "Khayyam Triangle". This is the same figure that penned the *Rubaiyat of Omar Khayyam*, a collection of poems popularized in the West when they were translated into English by Edward FitzGerald in 1859. These poems still remain a part of the English literary canon; I read them in an English Literature survey course when I was an undergraduate. It further underscores how our current boundaries between the sciences and the arts is a historical construction, and in past ages, these boundaries existed elsewhere, if at all. I demonstrated the fame of Khayyam's poems by showing a parody article *I Could Write A Better Rubaiyat Than That Khayyam Dipshit* from humor site *The Onion* (Fig. 2). The (fictional) op-ed ends with:

> *I just wish I could hop in a time machine and travel back to 12th Century Khorasan. I'd tell Khayyam to stick to math and astronomy, and leave the poetry to folks who have a friggin' clue.*

Surely the poems must have some notoriety to merit such profane parody.

Finally, the oldest claim goes to Pingala of India who lived somewhere between ~300 BC and ~200 BC. While this suggests that it should be called *Pingala's Triangle*, that phrase does not appear to be in popular usage. Nonetheless, it supersedes Pascal's claim by at least *1800 years*.

4 Euclid's Algorithm vs. The Chinese Remainder Theorem

The most significant historical confrontation I presented was the difference in naming conventions between *Euclid's Algorithm* and the *Chinese Remainder Theorem*. As a follow-up, I assigned them an optional bonus assignment where they could further investigate the topic. This aligned with pedagogical recommendations for the run-up to the 2020 US presidential election. We were warned that students might be distracted and unresponsive that week, and that assessing concept mastery in this environment would be compromised. Thus, I chose to give an optional assignment in lieu of a required problem set.

I will first describe the historical content, then the assignment, and finally the student's findings.

4.1 Euclid's Algorithm

4.1.1 Did Euclid Discover Euclid's Algorithm?

We covered an efficient algorithm for finding the greatest common divisor between two integers, known as *Euclid's Algorithm*. The question then naturally arises: did Euclid ($\sim$300 BC) discover this algorithm? While the algorithm itself appears in Book 7 and 10 of Euclid's *Elements*, modern scholarship is skeptical that he originated it. For example, André Weil in his book *Number Theory* (2001, Fig. 3, left) says the following:

> *It is generally agreed upon that much, if not all of the content of those books is of earlier origin, but little can be said about the history behind them.*

Donald Knuth, an early computer scientist pioneer (e.g. he joined Stanford Computer Science four years after its founding), also expresses skepticism in his widely-cited 1969 text *The Art of Computer Programming, Volume 2: Seminumerial Algorithms* (Fig. 4):

> *Euclid's algorithm is found in Book 7, Propositions 1 and 2 of his Elements (c. 300 B.C.), but it probably wasn't his own invention. Some scholars believe that the method was known up to 200 years earlier, at least in its subtractive form, and it was almost certainly known to Eudoxus (c. 375 B.C.); see K. von Fritz, Ann. Math. (2) 46 (1945), 242–264. Aristotle (c. 330 B.C.) hinted at it in his Topics, 158b, 29–35. However, very little hard evidence about such early history has survived [see W. R. Knorr, The Evolution of the Euclidean Elements (Dordrecht: 1975)].*

Nevertheless, Weil argues that since Euclid *popularized* this algorithm, the naming remains appropriate (Fig. 3, right)):

> *What matters for our purposes is that the very board diffusion of Euclid in later centuries, while driving out all earlier texts, made this body of knowledge widely available to mathematicians from then on.*

Thus, one naming standard is posited. Even if an author's *inventor* status cannot be entirely authenticated, the role of *popularizer* is also a useful one, and worthy of recognition.

4.1.2 How Long Has It Been Called Euclid's Algorithm?

A related question is: how long have scientists and mathematicians called it *Euclid's Algorithm*? Is it a recent phenomenon, or does it stretch back to antiquity? The oldest English usage I could find was by a math professor at the University of Chicago, Leonard Eugene Dickson, in his article *Finite Fields Whose Elements are Linear Differential Expressions* (1903, Fig. 5):

> *Euclid's algorithm for the greatest common divisor is seen to hold.*

A contemporaneous article from Saul Epsteen, *On Linear Differential Congruences* (1903, Fig. 6), uses a similar but not identical phrasing:

> *An algorithm analogous to Euclid's.*

Dickson and Epsteen were colleagues at the University of Chicago, and these two articles appear in the same journal issue. Was this phrase coined by two University of Chicago mathematicians in the 1900s, and only found its way into popular use because these two men happened to share offices on the same hallway at the turn of the 20th century?

To investigate further, I decided to ask the students if they could find older instances of the phrase. Spoiler: They found some.

4.2 The Chinese Remainder Theorem

4.2.1 Why Is It The *Chinese* Remainder Theorem?

The Chinese Remainder Theorem applies to a system of congruences, and comes with an algorithm for finding the solution to the system. (For more details, take the course.) It was natural to introduce this theorem immediately after Euclid's Algorithm, because it uses that algorithm as a building block.

The question then immediately arises: why is it the *Chinese* Remainder Theorem? There is an extensive discussion of this question on the website Math Overflow[2], where someone jokes that consistency seems to demand that *maybe we should call the Euclidean Algorithm the "European Algorithm" instead.* The joke poses a valid question: since when are theorems named after nationalities? No other instance comes to mind. One possible explanation is that the theorem was found in some ancient Chinese manuscripts of unknown authorship, and in the absence of better information, it was named after the place of its discovery.

This explanation is quickly dispelled; the provenance term can be traced quite precisely. Alexander Wylie (1815–1887), a British missionary to China, first introduced the Chinese Remainder Theorem to a Western audience in his nine-part series *Jottings on the Science of the Chinese*, published in the newspaper *The North China Herald* in 1853. After his death, these were compiled into the book *Chinese Researches* (1897). The relevant passage is on page 175 of that text (Fig. 7):

> *One of the most remarkable of these is the* Ta-yen *"Great Extension," a rule for the resolution of indeterminate problems This rule is met with in embryo in Sun-Tsze's Arithmetical Classic under the name of the* Wuh-puh-chi-soo*, "Unknown Numerical Quantities" where after a general statement in four lines of rhyme the following question is proposed:*

Immediately afterwards, an instance of a system of congruences is presented, and the Chinese Remainder Theorem is described. The author, Sun-Tsze ($\sim$400 AD), is named directly[3].

Like in the case of Euclid, Wylie expresses some misgivings that Sun-Tsze is the original discoverer of the theorem, as he observes in the immediately preceding text (Fig. 7):

> *To examining the productions of the Chinese one finds considerable difficulty in assigning the precise date for the origin of any mathematical process for on almost every point where we consult a native author we find references to some still earlier work on the subject. The high veneration with which it has been customary for them to look upon the labours of the ancients has made them more desirous of elucidating the works of their predecessors than of seeking fame in an untrodden path; so that some of their most important formulae have reached the state in which we now find them by an almost innumerable series of increments.*

In modern language, Wylie found it difficult to separate the Related Works section from the Novel Contributions section. Still, if we are using the relaxed standard of *popularizer* instead of *inventor*, why is it not called the *Sun-Tsze* Remainder Theorem?

4.2.2 How Long Has It Been Called the Chinese Remainder Theorem?

Wylie's work described the theorem, but never used the exact phrase "Chinese Remainder Theorem," so further investigation is needed. Starting from the references in the Math Overflow article, I searched for the first usage of that exact phrase. Again, Leonard Eugene Dickson, the University of Chicago mathematician, appears almost immediately. In his 1920 book *History of the Theory of Numbers, Vol. II: Diophantine Analysis* (Fig. 8), he refers to the "Chinese Problem of Remainders", restates the theorem, and directly cites Wylie as his source. The phrasing is close, but not an exact match. The phrase "Chinese remainder theorem" first

[2] `https://mathoverflow.net/questions/11951/what-is-the-history-of-the-name-chinese-remainder-theorem`

[3] His name is sometimes written as Sun Tzu, but should not be confused with the author of *The Art of War* from $\sim$500 BC.

appears in Dickson's 1929 article *The Forms* $ax^2 + by^2 + cz^2$ *Which Represent All Integers* (Fig. 9). Even then, the lower-case *r*emainder and *t*heorem indicates that the term has not yet been codified as a proper noun.

The first proper noun form usage appears to be in 1931 by Ralph Sylvester Underwood in his article *On Universal Quadratic Null Forms in Five Variables* (Fig. 10):

> *By the Chinese Remainder Theorem there exists integers* z, w, v *such that ...*

Once again, Underwood was a mathematician at the University of Chicago. He was clearly aware of Dickson, as the article opens with (Fig. 11)

> *1. We shall use L. E. Dickson's result:*

We are faced with a question similar to the naming of *Euclid's Algorithm*. Was this seemingly ancient-looking phrase actually coined by a few University of Chicago professors **less than 100 years ago?**

As with the case of Euclid's Algorithm, I asked students to find an older occurrence of this phrase. No verifiable instances of an older usage were found. This may in fact be the origin of the term.

4.2.3 What Did *Chinese* Mean in 1929?

Why did Dickson choose to call it the *Chinese* Remainder Theorem when the inventor/popularizer's name Sun-Tsze was immediately available to him? We can never know what was in his mind in 1929, but we can examine the environment that surrounded him. This issue of naming was of immediate relevance to the class, as it was occurring against the backdrop of COVID-19 being called the "Chinese Virus" the "Wuhan Virus" and "Kung Flu" by President Donald Trump.

As I was assembling these lectures, I was introduced to Professor Mary Lui, an expert from Yale's Department of History, who pointed me to *The Chinese Exclusion Act*, a documentary that she had helped create for the PBS show *American Experience*[4]. Based on this documentary, I attempted to characterize the environment in which Dickson chose this name by presenting the surrounding events in the United States.

- **1882**: Five years before Wylie's death, the US passes the *Chinese Exclusion Act*, barring all Chinese immigrants from entering the country. This is the *only* time in US history that a specific nationality is singled out and prohibited from immigrating into the country.

  There are very few Chinese-Americans in the US in 1882, but the larger symbolic test is to see if the post-Civil War Reconstruction era is ending, and if it is politically viable to begin stripping minorities of their civil rights. The act establishes the viability, and a wave of racial violence begins.

- **1885**: Both Tacoma, Washington and Eureka, California expel all of their Chinese residents and pass laws declaring that *no* Chinese immigrants can legally live within city limits. In Eureka, the law stays on the books until 1950.

  Elsewhere in the American West, tensions between white and Chinese gold miners have been rising for years, and boil over in the *Rock Springs Massacre*, where a group of white miners burn down Chinatown in Rock Springs and murder 28 Chinese miners. Several participants are arrested and later freed. No convictions are ever made.

- **1887:** The mutilated bodies of 34 Chinese gold miners are found floating down the Snake River in Oregon. The *Snake River Massacre* has occurred further upstream, and so many bodies were tossed into the river that remains are discovered for years afterwards. Again, no convictions are ever made.

[4] https://www.pbs.org/wgbh/americanexperience/films/chinese-exclusion-act/#part01

- **1892:** The *Chinese Exclusion Act* is renewed, and made even more restrictive. Now even existing Chinese immigrants are required to carry a *photo ID* at all times. In what may be the largest act of mass civil disobedience in US history, over 100,000 Chinese immigrants refuse to comply, and take a lawsuit all the way to the Supreme Court. They lose.
- **1897:** Alexander Wylie's *Chinese Researches* is published.
- **1904:** The *Chinese Exclusion Act* is made permanent. It no longer needs to be renewed every 10 years.
- **1917:** The *Chinese Exclusion Act* is expanded into the *Asiatic Barred Zone Act*, establishing strict immigration quotas from all countries west of Turkey and east of Japan.
- **1920:** Dickson publishes *History of the Theory of Numbers, Vol. II: Diophantine Analysis*.
- **1921:** The *Emergency Quota Act* is passed, which sets strict quotas on immigrants from southern and eastern Europe, including countries such as Italy. By the process of elimination, western and northern Europeans are now the only preferred immigrants. This prejudice is visible in movies like *The Godfather* (1972) where Italian immigrants are treated as second-class citizens in 1940s New York City.
- **1924:** The *Asian Exclusion Act* is passed, reducing the quotas established by the *Asiatic Barred Zone Act* to zero. The project started by the *Chinese Exclusion Act* is now complete. All Asian immigrants are officially barred from entering the US.
- **1929:** Dickson first uses the phrase *Chinese remainder theorem*.

  What did the term "Chinese" mean to him? Was his usage an act of resistance, openly acknowledging the contribution of an ostracized minority? Or does the removal of Sun-Tsze's name reflect the prejudices of the time, where all Chinese were lumped into an undifferentiated and inscrutable mass?

Ending the timeline here is too grim, and not seeing how these events extend forward is profoundly unsatisfying. I extended the timeline through the present day.

- **1943:** The *Magnuson Act* passes during World War II in response to Japanese propaganda accusing the US of hypocrisy: How can it be "Land of the Free, Home of the Brave" when those freedoms do not extend to Asians? For the first time in 61 years, Chinese people are allowed to immigrate into the US. They are limited to the strict, minuscule numbers enumerated in the 1924 *Asian Exclusion Act*, but this is still a victory, because the number is no longer zero.
- **1965:** The *Hart-Cellar Act* passes during the Cold War in response to Russian propaganda accusing the US of perpetuating the same hypocrisies. This is the act that finally re-opens the doors to large-scale Asian immigration into the US.

  This act passes in the middle of the Civil Rights Movement. This is the same year as the March on Selma, the same year that a state trooper fractures John Lewis's skull on the Edmund Pettrus Bridge, and the same year as the *Voting Rights Act*. Medgar Evers was assassinated two year prior, Malcolm X just eight months before, and Dr. King will be shot in Memphis three years later.

  The language of the *Hart-Cellar Act* specifically favors visas for (Fig. 12)

  > *members of the professions, or who because of their exceptional ability in the sciences or the arts will substantially benefit prospectively the national economy, cultural interests, or welfare of the United States.*

> This sets the stage for a wave of doctors, scientists, and engineers to arrive from Asia. They are the parents and grandparents of Yale students and faculty, including many in this class. It also establishes a professional class of Asian-Americans with "model minority" status, leading to the current lawsuit by President Trump's Department of Justice which accuses Yale of discriminatory admissions policies.

Finally, the *Hart-Cellar Act* allows my uncle to immigrate from South Korea in 1966. My mother arrives six years after that, her skills as a nutritionist allowing her to secure a visa. My father arrives a year later to pursue a Ph.D. in Mechanical Engineering. And that is how I came to be here now, teaching this course, and writing this document.

5 Election Week Bonus Assignment

5.1 Candidate Topics

To follow up on this material, I assigned an optional bonus assignment for the week before the 2020 US Presidential Election. The assignment handout is provided at the very end of this document. To summarize, they could investigate any of the following topics:

1. Find an English appearance of the common noun form *Chinese remainder theorem* prior to 1929.
2. Find an English appearance of the proper noun form *Chinese Remainder Theorem* prior to 1931.
3. Find an appearance, in any language, of *Euclid's Algorithm* or *Euclidean Algorithm* prior to 1903.
4. Find what other terms are used in China for the *Chinese Remainder Theorem*.

36 out of 80 students chose to attempt this assignment, and their findings are as follows.

5.2 *Chinese Remainder Theorem* As Common or Proper Noun

None of the students were able to find an instance of *Chinese remainder theorem* prior to 1929 or *Chinese Remainder Theorem* prior to 1931. This is not definitive proof that instances do not exist, but the fact that they were able to find older examples of *Euclid's Algorithm* does give the argument further weight.

5.3 *Euclid's Algorithm* Prior to 1903

Many instances of the phrase *Euclid's Algorithm*, or a close approximation in another language, were found. In the following, I have anonymized the student's names, because while they agreed to have their names shared internally to Yale's Poorvu Center for Teaching and Learning, but I didn't secure their permission (yet) to disclose their identities to the wider Internet.

- Students A, B and C found *Über Eisensteins Beweis des quadratischen Reciproeitätsgesetzes* by Ernst Fischer (1900).
- D found *Algebra mit Einschluss der elementaren Zahlentheorie* by Otto Pund (1899).
- E found a review of *Weber's Algebra* by James Pierpoint (1897).
- F and G found *Euklidischen Algorithmus* by Felix Klein (1896).
- H found *Biographical Studies: On Number Theory* by Thomas Joannes Stieltjes (1890).
- I, J, and K found *Sur Une Notion Oui Comprend Celle De La Divisibilité Et Sur La Théorie Générale De L'élimination* by Jules Molk (1883). As this was the oldest reference found, I announced them in class as **the winners!**

5.4 Other Terms In China For *Chinese Remainder Theorem*

Many students found Chinese texts that do in fact refer to the *Chinese Remainder Theorem* as *Sun Tsze's Theorem*. Thus, despite Wylie's misgivings, the standard of naming the theorem after the popularizer has been applied in China. Some additional wrinkles were also discovered:

- L found two instances where the term *Sun Tsze Theorem* was quickly followed by *foreign scholars often call it the Chinese Remainder Theorem* and *foreigners call it the Chinese Remainder Theorem*. Some tension is visible in the use of this naming convention.
- M found that term *Han Xin Dian Bing* is also used, presumably after General Han Xin.
- N found that in the Baidu Encyclopedia, the term *Sun Tsze's Theorem* is almost one hundred times more popular than *Chinese Remainder Theorem*, suggesting that the former is more popular on mainland China.

  The opposite pattern appears on Chinese language Wikipedia, where the term *Chinese Remainder Theorem* is ten times more popular. As Wikipedia is blocked in mainland China, this presumably reflects the preferences of Taiwanese users. Usage patterns may fall along political lines.

6 Closing Thoughts

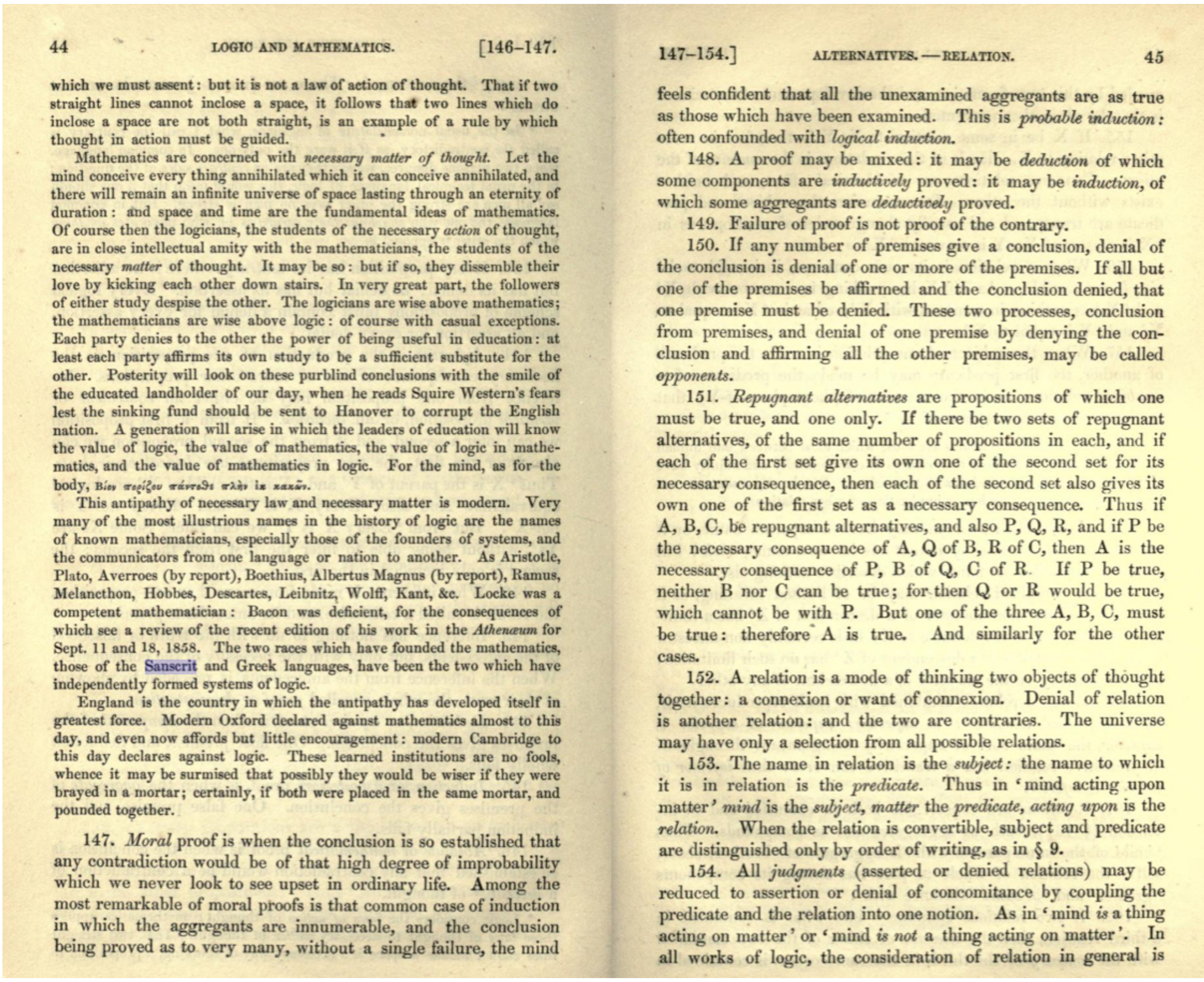
Collecting and presenting much of this material was very mentally demanding, especially material surrounding large-scale racial violence in immigrant communities. I would not suggest that instructors in compromised personal or professional situations make a similar attempt; in particular I never would have made such an attempt before tenure. That being said, finding historical material to widen past the Euro-centric lens was not difficult. Others have investigated these histories, and starting from the "Historical Development" sections on Wikipedia for any given math concept yields numerous promising citations. Following those citations, accessing primary source material through the Yale Library, and investigating further, is both interesting and straightforward. The main barrier to further curriculum development is time, not lack of material.

I had misgivings that I would be ambushing students with this material in a supposedly sterile technical class, especially since the news was already saturated with similar material. I did not receive any explicit negative feedback, but it is still hard to know how the material was received, especially when mediated through Zoom. The historical material did not have a major positive or negative impact on course evaluations. My end-of-course numerical ratings did not skew significantly from the global averages for the major and the college. Some written comments were very positive about the historical material, while a handful complained that a technical course should stick to technical material.

All of this material was presented as an addendum to the existing technical material. It was not integrated into the evaluation, and no demonstration of mastery was expected. It is not clear if student evaluation is necessary; the point was to push back on Euro-centric presentations of the material, not the material itself. Still, future iterations should find a way to measure the impact of this material in terms of learning outcomes and student retention in the major.

Finally, a larger teaching project may be possible. Political factors have led to certain math topics becoming well-developed, such as numerical methods for hydrogen bombs, or statistical methods for reconnoitering faces, while others have been relatively neglected. The converse also occurs, such as G.H. Hardy researching number theory specifically because he believed that it had no practical applications, only to have it later weaponized into military encryption. However, investigating these possibilities was outside the scope of this course.

7 Original Source Materials



44 LOGIC AND MATHEMATICS. [146–147.

which we must assent: but it is not a law of action of thought. That if two straight lines cannot inclose a space, it follows that two lines which do inclose a space are not both straight, is an example of a rule by which thought in action must be guided.

Mathematics are concerned with *necessary matter of thought.* Let the mind conceive every thing annihilated which it can conceive annihilated, and there will remain an infinite universe of space lasting through an eternity of duration: and space and time are the fundamental ideas of mathematics. Of course then the logicians, the students of the necessary *action* of thought, are in close intellectual amity with the mathematicians, the students of the necessary *matter* of thought. It may be so: but if so, they dissemble their love by kicking each other down stairs. In very great part, the followers of either study despise the other. The logicians are wise above mathematics; the mathematicians are wise above logic: of course with casual exceptions. Each party denies to the other the power of being useful in education: at least each party affirms its own study to be a sufficient substitute for the other. Posterity will look on these purblind conclusions with the smile of the educated landholder of our day, when he reads Squire Western's fears lest the sinking fund should be sent to Hanover to corrupt the English nation. A generation will arise in which the leaders of education will know the value of logic, the value of mathematics, the value of logic in mathematics, and the value of mathematics in logic. For the mind, as for the body, Βίον πορίζου πάντοθι πλὴν ἐκ κακῶν.

This antipathy of necessary law and necessary matter is modern. Very many of the most illustrious names in the history of logic are the names of known mathematicians, especially those of the founders of systems, and the communicators from one language or nation to another. As Aristotle, Plato, Averroes (by report), Boethius, Albertus Magnus (by report), Ramus, Melancthon, Hobbes, Descartes, Leibnitz, Wolff, Kant, &c. Locke was a competent mathematician: Bacon was deficient, for the consequences of which see a review of the recent edition of his work in the *Athenæum* for Sept. 11 and 18, 1858. The two races which have founded the mathematics, those of the Sanscrit and Greek languages, have been the two which have independently formed systems of logic.

England is the country in which the antipathy has developed itself in greatest force. Modern Oxford declared against mathematics almost to this day, and even now affords but little encouragement: modern Cambridge to this day declares against logic. These learned institutions are no fools, whence it may be surmised that possibly they would be wiser if they were brayed in a mortar; certainly, if both were placed in the same mortar, and pounded together.

147. *Moral* proof is when the conclusion is so established that any contradiction would be of that high degree of improbability which we never look to see upset in ordinary life. Among the most remarkable of moral proofs is that common case of induction in which the aggregants are innumerable, and the conclusion being proved as to very many, without a single failure, the mind

147–154.] ALTERNATIVES.—RELATION. 45

feels confident that all the unexamined aggregants are as true as those which have been examined. This is *probable induction:* often confounded with *logical induction.*

148. A proof may be mixed: it may be *deduction* of which some components are *inductively* proved: it may be *induction*, of which some aggregants are *deductively* proved.

149. Failure of proof is not proof of the contrary.

150. If any number of premises give a conclusion, denial of the conclusion is denial of one or more of the premises. If all but one of the premises be affirmed and the conclusion denied, that one premise must be denied. These two processes, conclusion from premises, and denial of one premise by denying the conclusion and affirming all the other premises, may be called *opponents.*

151. *Repugnant alternatives* are propositions of which one must be true, and one only. If there be two sets of repugnant alternatives, of the same number of propositions in each, and if each of the first set give its own one of the second set for its necessary consequence, then each of the second set also gives its own one of the first set as a necessary consequence. Thus if A, B, C, be repugnant alternatives, and also P, Q, R, and if P be the necessary consequence of A, Q of B, R of C, then A is the necessary consequence of P, B of Q, C of R. If P be true, neither B nor C can be true; for then Q or R would be true, which cannot be with P. But one of the three A, B, C, must be true: therefore A is true. And similarly for the other cases.

152. A relation is a mode of thinking two objects of thought together: a connexion or want of connexion. Denial of relation is another relation: and the two are contraries. The universe may have only a selection from all possible relations.

153. The name in relation is the *subject:* the name to which it is in relation is the *predicate.* Thus in 'mind acting upon matter' *mind* is the *subject*, *matter* the *predicate*, *acting upon* is the *relation.* When the relation is convertible, subject and predicate are distinguished only by order of writing, as in § 9.

154. All *judgments* (asserted or denied relations) may be reduced to assertion or denial of concomitance by coupling the predicate and the relation into one notion. As in 'mind *is* a thing acting on matter' or 'mind *is not* a thing acting on matter'. In all works of logic, the consideration of relation in general is

Figure 1: Page 44 of Augustus De Morgan's *Syllabus of a Proposed System of Logic* (1860).

THE ONION | THE A.V. CLUB DEADSPIN GIZMODO JALOPNIK JEZEBEL KOTAKU LIFEHACKER THE ROOT THE TAKEOUT | THE INVENTORY

the ONION® | America's Finest News Source.

Shop

HOME LATEST POLITICS SPORTS LOCAL ENTERTAINMENT THE TOPICAL OGN OPINION

COMMENTARY

I Could Write A Better Rubaiyat Than That Khayyam Dipshit

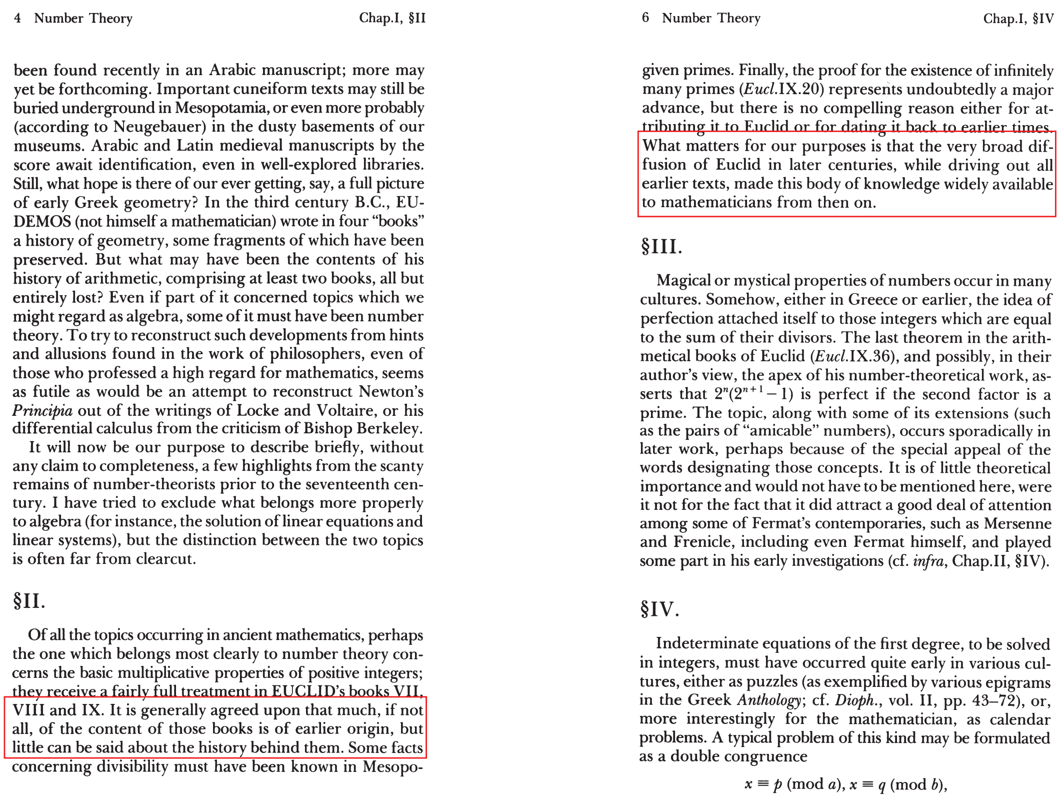
Gord Hunsacker
8/01/01 3:00PM • SEE MORE: OPINION

Gord Hunsacker

Down at the loading dock, me and the guys get into a lot of good-natured scraps about sports teams and movies and whatnot. Sure, it gets a little heated sometimes, but it's always in good fun. When it comes to poetry, though, there are days when I just want to haul off and punch their sorry faces.

Especially Tony. I mean, he's entitled to his opinion and all, and if he doesn't acknowledge that Keats was the greatest English poet of the 19th century, that doesn't make him evil or nothing. But when he starts mouthing off about *The Rubaiyat Of Omar Khayyam* being one of the five greatest poems ever, I want

Figure 2: `https://www.theonion.com/i-could-write-a-better-rubaiyat-than-that-khayyam-dipsh-1819583837`.



4 Number Theory Chap.I, §II

been found recently in an Arabic manuscript; more may yet be forthcoming. Important cuneiform texts may still be buried underground in Mesopotamia, or even more probably (according to Neugebauer) in the dusty basements of our museums. Arabic and Latin medieval manuscripts by the score await identification, even in well-explored libraries. Still, what hope is there of our ever getting, say, a full picture of early Greek geometry? In the third century B.C., EUDEMOS (not himself a mathematician) wrote in four "books" a history of geometry, some fragments of which have been preserved. But what may have been the contents of his history of arithmetic, comprising at least two books, all but entirely lost? Even if part of it concerned topics which we might regard as algebra, some of it must have been number theory. To try to reconstruct such developments from hints and allusions found in the work of philosophers, even of those who professed a high regard for mathematics, seems as futile as would be an attempt to reconstruct Newton's *Principia* out of the writings of Locke and Voltaire, or his differential calculus from the criticism of Bishop Berkeley.

It will now be our purpose to describe briefly, without any claim to completeness, a few highlights from the scanty remains of number-theorists prior to the seventeenth century. I have tried to exclude what belongs more properly to algebra (for instance, the solution of linear equations and linear systems), but the distinction between the two topics is often far from clearcut.

§II.

Of all the topics occurring in ancient mathematics, perhaps the one which belongs most clearly to number theory concerns the basic multiplicative properties of positive integers; they receive a fairly full treatment in EUCLID's books VII, VIII and IX. It is generally agreed upon that much, if not all, of the content of those books is of earlier origin, but little can be said about the history behind them. Some facts concerning divisibility must have been known in Mesopo-

6 Number Theory Chap.I, §IV

given primes. Finally, the proof for the existence of infinitely many primes (*Eucl.*IX.20) represents undoubtedly a major advance, but there is no compelling reason either for attributing it to Euclid or for dating it back to earlier times. What matters for our purposes is that the very broad diffusion of Euclid in later centuries, while driving out all earlier texts, made this body of knowledge widely available to mathematicians from then on.

§III.

Magical or mystical properties of numbers occur in many cultures. Somehow, either in Greece or earlier, the idea of perfection attached itself to those integers which are equal to the sum of their divisors. The last theorem in the arithmetical books of Euclid (*Eucl.*IX.36), and possibly, in their author's view, the apex of his number-theoretical work, asserts that $2^n(2^{n+1}-1)$ is perfect if the second factor is a prime. The topic, along with some of its extensions (such as the pairs of "amicable" numbers), occurs sporadically in later work, perhaps because of the special appeal of the words designating those concepts. It is of little theoretical importance and would not have to be mentioned here, were it not for the fact that it did attract a good deal of attention among some of Fermat's contemporaries, such as Mersenne and Frenicle, including even Fermat himself, and played some part in his early investigations (cf. *infra*, Chap.II, §IV).

§IV.

Indeterminate equations of the first degree, to be solved in integers, must have occurred quite early in various cultures, either as puzzles (as exemplified by various epigrams in the Greek *Anthology*; cf. *Dioph.*, vol. II, pp. 43–72), or, more interestingly for the mathematician, as calendar problems. A typical problem of this kind may be formulated as a double congruence

$$x \equiv p \pmod{a},\ x \equiv q \pmod{b},$$

Figure 3: Page 4 and 6 of André Weil's *Number Theory* (2001).

Euclid's algorithm. Although Eq. (6) is useful for theoretical purposes, it is generally no help for calculating a greatest common divisor in practice, because it requires that we first determine the canonical factorization of u and v. There is no known way to find the prime factors of an integer very rapidly (see Section 4.5.4). But fortunately the greatest common divisor of two integers can be found efficiently without factoring, and in fact such a method was discovered more than 2250 years ago; it is *Euclid's algorithm*, which we have already examined in Sections 1.1 and 1.2.1.

Euclid's algorithm is found in Book 7, Propositions 1 and 2 of his *Elements* (c. 300 B.C.), but it probably wasn't his own invention. Some scholars believe that the method was known up to 200 years earlier, at least in its subtractive form, and it was almost certainly known to Eudoxus (c. 375 B.C.); see K. von Fritz, *Ann. Math.* (2) **46** (1945), 242–264. Aristotle (c. 330 B.C.) hinted at it in his *Topics*, 158b, 29–35. However, very little hard evidence about such early history has survived [see W. R. Knorr, *The Evolution of the Euclidean Elements* (Dordrecht: 1975)].

Figure 4: From Donald Knuth's *The Art of Computer Programming, Volume 2: Seminumerial Algorithms* (1969).

FIELDS WHOSE ELEMENTS ARE LINEAR DIFFERENTIAL EXPRESSIONS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, April 25, 1903.)

A. GULDBERG * has considered expressions of the form

$$Ay = a_\alpha \frac{d^\alpha y}{dx^\alpha} + a_{\alpha-1}\frac{d^{\alpha-1}y}{dx^{\alpha-1}} + \cdots + a_1 \frac{dy}{dx} + a_0 y,$$

in which $a_\alpha, \cdots, a_0$ are integers taken modulo p, p being a prime number. The *product* $Ay \cdot By$ of two such expressions in defined by Boole's symbolic method † to be

$$\left(a_\alpha \frac{d^\alpha}{dx^\alpha} + \cdots + a_1 \frac{d}{dx} + a_0\right)\left(b_\beta \frac{d^\beta}{dx^\beta} + \cdots + b_1 \frac{d}{dx} + b_0\right)y,$$

so that the expansion may be effected as if d/dx were a constant. If, in this manner, $Ay \cdot By \equiv Cy \pmod p$, we say that Ay and By are *divisors* modulo p of Cy. Euclid's algorithm for the greatest common divisor is seen to hold. We may therefore define reducible and irreducible differential expressions modulo p. Let

$$\Delta y = \delta_n \frac{d^n y}{dx^n} + \cdots + \delta_1 \frac{dy}{dx} + \delta_0 y$$

* "Sur des congruences différentielles linéaires," *Comptes rendus*, vol. 125, p. 489 (1897).
† Boole, Differential Equations, p. 381, seq.

Figure 5: From L.E. Dickson's *Finite Fields Whose Elements are Linear Differential Expressions* (1903).

§ 1.

This section is mainly a summary of Guldberg's results. We consider linear differential forms with integral coefficients

$$D(y) = Dy = \sum_{i=0}^{n} a_i \frac{d^i y}{dx^i}$$

and agree to understand the word "product" in the well known symbolic sense of Boole.*

If $D_1 y = D_2 y + p \cdot D_3 y$, then we may write the congruence $D_1 y \equiv D_2 y \pmod{p}$. When a differential expression Dy is given, we first reject the terms whose coefficients are multiples of p, then if $Dy = D_1 y \cdot D_2 y \pmod{p}$, we say that $D_1 y$ and $D_2 y$ are divisors of Dy modulo p.

In one and only in one of the *associated* forms $1\ D$, $2\ D$, $3\ D$, $\cdots$, $(p-1)D$ is the coefficient of the term of highest order congruent to 1 modulo p. This one is called the *principal* form.

A form D which is not divisible by other differential forms (except by its associated forms) is said to be *irreducible* or *prime* modulo p.

An algorithm analogous to Euclid's for finding the greatest common divisor holds † and from this it can be shown that: Any Dy (or simply D) can be decomposed in one and only one way into the product of an integer and irreducible principal forms.

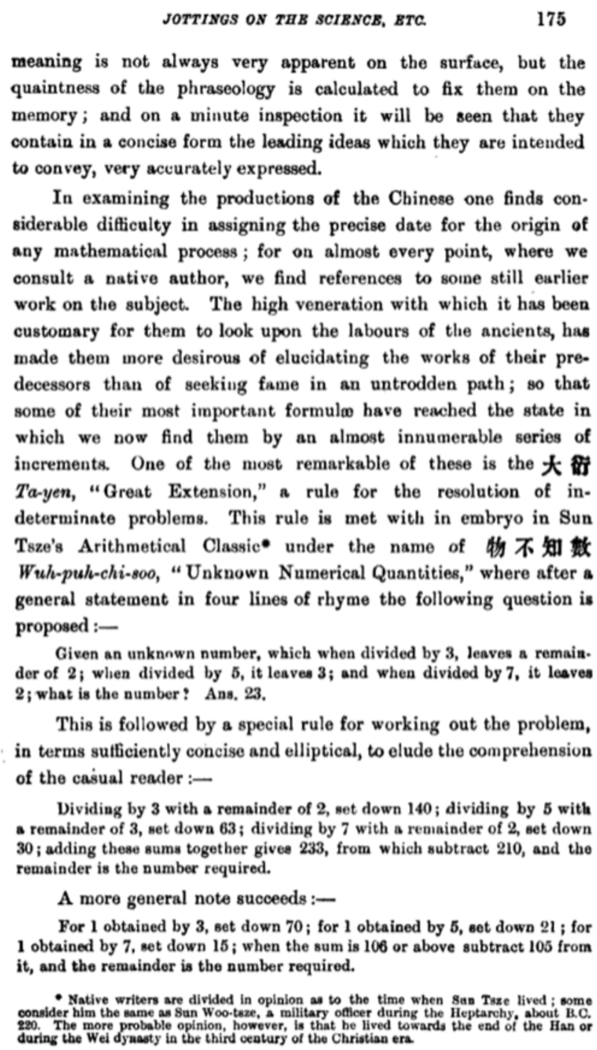
The fact that D is divisible by Δ, modulo p can be expressed thus: $D \equiv 0$ (modd p, Δ), which means that $D = \phi \cdot \Delta + p \cdot D_1$. Likewise $D_1 \equiv D_2$ (modd p, Δ) means that $D_1 = \phi \cdot \Delta + pD_3 + D_2$. If Δ is of order n, any form D is congruent to one and only one of the p^n forms

$$\sum_{0}^{n-1} a_i \frac{d^i y}{dx^i}$$

* Boole's Differential Equations, p. 381.

† Although Guldberg's conclusions are correct in a general sort of way his notation is not always so, he does not seem to notice that in this theory integers cannot appear by themselves, but are always accompanied by y or a derivative of y (zero excepted). See also the correction at the end of this section.

Figure 6: From Saul Epsteen's *On Linear Differential Congruences* (1903).



JOTTINGS ON THE SCIENCE, ETC. 175

meaning is not always very apparent on the surface, but the quaintness of the phraseology is calculated to fix them on the memory; and on a minute inspection it will be seen that they contain in a concise form the leading ideas which they are intended to convey, very accurately expressed.

In examining the productions of the Chinese one finds considerable difficulty in assigning the precise date for the origin of any mathematical process; for on almost every point, where we consult a native author, we find references to some still earlier work on the subject. The high veneration with which it has been customary for them to look upon the labours of the ancients, has made them more desirous of elucidating the works of their predecessors than of seeking fame in an untrodden path; so that some of their most important formulæ have reached the state in which we now find them by an almost innumerable series of increments. One of the most remarkable of these is the 大衍 *Ta-yen*, "Great Extension," a rule for the resolution of indeterminate problems. This rule is met with in embryo in Sun Tsze's Arithmetical Classic* under the name of 物不知數 *Wuh-puh-chi-soo*, "Unknown Numerical Quantities," where after a general statement in four lines of rhyme the following question is proposed:—

Given an unknown number, which when divided by 3, leaves a remainder of 2; when divided by 5, it leaves 3; and when divided by 7, it leaves 2; what is the number? Ans. 23.

This is followed by a special rule for working out the problem, in terms sufficiently concise and elliptical, to elude the comprehension of the casual reader:—

Dividing by 3 with a remainder of 2, set down 140; dividing by 5 with a remainder of 3, set down 63; dividing by 7 with a remainder of 2, set down 30; adding these sums together gives 233, from which subtract 210, and the remainder is the number required.

A more general note succeeds:—

For 1 obtained by 3, set down 70; for 1 obtained by 5, set down 21; for 1 obtained by 7, set down 15; when the sum is 106 or above subtract 105 from it, and the remainder is the number required.

* Native writers are divided in opinion as to the time when Sun Tsze lived; some consider him the same as Sun Woo-tsze, a military officer during the Heptarchy, about B.C. 220. The more probable opinion, however, is that he lived towards the end of the Han or during the Wei dynasty in the third century of the Christian era.

Figure 7: Page 175 from from Alexander Wylies *Chinese Researches* (1897).

J. G. Zehfuss[68] gave the formula of Cauchy[60] and noted that, if $\mu = \alpha^m \beta^n \cdots$, and if A is not divisible by the prime α, B not by β, $\cdots$, then

$$\left(\frac{A\mu}{\alpha^m}\right)^{(\alpha-1)\alpha^{m-1}} + \left(\frac{B\mu}{\beta^n}\right)^{(\beta-1)\beta^{n-1}} + \cdots \equiv 1 \pmod{\mu}.$$

For $A = B = \cdots = a$, let the left member become k. Then $ax \equiv b \pmod{\mu}$ has the root kb/a. It also has the root $(1 - AB\cdots)b/a$, where

$$A = \left(1 + a\frac{(\alpha-1)!}{a_\alpha}\right)^m \equiv 0 \pmod{\alpha^m},$$

$$B = \left(1 + a\frac{(\beta-1)!}{a_\beta}\right)^n \equiv 0 \pmod{\beta^n}, \quad \cdots,$$

where a_α is the least positive residue of a modulo α, since, by Wilson's theorem, $a_\alpha + (\alpha - 1)!\,a$ is divisible by the prime α.

M. F. Daniëls[69] noted that, if $\rho_1 \cdots \rho_n \equiv \pm 1 \pmod{k}$ by Wilson's generalized theorem, then $\rho_i x \equiv 1 \pmod{k}$ has the root $\pm \rho_1 \cdots \rho_{i-1} \rho_{i+1} \cdots \rho_n$. Further, if $k = p^\nu q^\mu \cdots$ and if $ac_1 \equiv 1 \pmod{p}$, $ac_2 \equiv 1 \pmod{q}$, $\cdots$, then $ax \equiv 1 \pmod{k}$ has the root

$$x = \frac{1}{a}\{1 - (1 - ac_1)^\nu (1 - ac_2)^\mu \cdots\}.$$

J. Perott[70] noted that if a and u are relatively prime and if a belongs to the exponent t modulo u, $ax \equiv 1 \pmod{u}$ has the unique solution $x \equiv a^{t-1} \pmod{u}$. He admitted he was anticipated by Cauchy.

CHINESE PROBLEM OF REMAINDERS.

Sun-Tsŭ,[71] in a Chinese work Suan-ching (arithmetic), about the first century A.D., gave in the form of an obscure verse a rule called t'ai-yen (great generalisation) to determine a number having the remainders 2, 3, 2, when divided by 3, 5, 7, respectively. He determined the auxiliary numbers 70, 21, 15, multiples of $5\cdot 7$, $3\cdot 7$, $3\cdot 5$ and having the remainder 1 when divided by 3, 5, 7, respectively. The sum $2\cdot 70 + 3\cdot 21 + 2\cdot 15 = 233$ is one answer. Casting out a multiple of $3\cdot 5\cdot 7$ we obtain the least answer 23. The rule became known in Europe through an article, "Jottings on the science of Chinese arithmetic," by Alexander Wylie,[72] a part of which was translated into German by K. L. Biernatzki.[73] A faulty rendition by

[68] Diss. (Heidelberg), Darmstadt, 1857; Archiv Math. Phys., 32, 1859, 422.
[69] Lineaire Congruenties, Diss., Amsterdam, 1890, 114, 90.
[70] Bull. des Sc. Math., (2), 17, I, 1893, 73–4.
[71] Y. Mikami, Abh. Geschichte Math. Wiss., 30, 1912, 32.
[72] North China Herald, 1852; Shanghai Almanac for 1853. Cf. remark by G. Vacca, Bibliotheca Math., (3), 2, 1901, 143; H. Cordier, Jour. Asiatic Soc., (2), 19, 1887, 358.
[73] Jour. für Math., 52, 1856, 59–94. French transl. by O. Terquem, Nouv. Ann. Math., (2), 1, 1862 (Bull. Bibl. Hist.), 35–44; 2, 1863, 529–540; and by J. Bertrand, Journal des Savants, 1869. Cf. Matthiessen.[79]

Figure 8: Page 57 from from L.E. Dickson's *History of the Theory of Numbers, Vol. II: Diophantine Analysis* (1920).

No two of a, b, c are even. Let us set $a=2A$, $b=2B$. By the preceding result, A and B are odd. Also, c is odd. If $A=4n-1$, we use $-f$ in place of f. Hence let $A=4n+1$. Then $f\equiv 2x^2+2By^2+cz^2 \pmod 8$. Consider only odd residues of f. Then $cz^2\equiv c \pmod 8$. The residues of $2x^2+2By^2$ are 0, 2, $2B$, $2B+2$. When these are increased by c, the sums must give the four odd residues modulo 8. Hence no two are congruent. Thus no two of 0, 1, B, $B+1$ are congruent modulo 4. Since B is odd and $\not\equiv 1 \pmod 4$, $B\equiv 3$, $B+1\equiv 0$, a contradiction.

This completes the proof of property III. Properties II and III imply the following property.

V. *a, b, c are relatively prime in pairs.*

Thus $cd\equiv -b \pmod a$ has a solution d which is prime to a. Suppose that d were a quadratic non-residue of an odd prime factor p of a. Write $a=pA$. Consider values of x, y, z for which f is divisible by p. Then $z^2\equiv dy^2 \pmod p$, whence y and z are divisible by p. Hence $f=pF$, where $F\equiv Ax^2 \pmod p$. Evidently Ax^2 takes at most $1+\frac{1}{2}(p-1)$ values incongruent modulo p. Hence there is an integer N that is not congruent to one of them. Thus f fails to represent $p(N+pw)$ for any value of w. This contradiction proves that $v^2\equiv d \pmod p$ is solvable. The usual induction shows that it is solvable modulo p^n. Also, $d^2\equiv d \pmod 2$. By means of the Chinese remainder theorem, we see that $w^2\equiv d$ (mod a, is solvable whether a is odd or double an odd integer,

Figure 9: Page 56 from from L.E. Dickson's *The Forms* $ax^2+by^2+cz^2$ *Which Represent All Integers* (1929).

744 R. S. UNDERWOOD [July

modulo ga if solvable modulis qs, r and t. It is solvable modulis qs and r in the four-* and hence the five-variable case. It remains to consider

$$F = G(ty). \tag{10}$$

Let t be the product of powers p^n of distinct primes. We shall use the following theorem:

THEOREM 2. *If for each factor* p^n *of* $t = p_1^{n_1} \cdots p_r^{n_r}$,

(11) $F \equiv G(p^n)$, *with* F *as in* (1) *and* (2), *has a solution* $z, w, v, y = \eta$, *with* $\eta = 1$ *or* π, *where*

(12) π *is an odd prime dividing no one of* g, a, d, α, h, *and not dividing one of* $N = j^2 - 4hl$, $M = A^2 - 4\alpha hC$, $P = 2hB - jA$, *then* (10) *is solvable with* y *odd but not necessarily the same as in the solution of* (11).

Note that by the last paragraph of §1

(13) one of $N, M, P \neq 0$.

First we prove

LEMMA 2A. *The congruence*

(14) $F \equiv G(\pi)$, π *as in* (12), *is solvable with* $y = k\pi$, *where* k *is an arbitrary integer*.

For, dropping the terms of F containing y, and multiplying (14) by $4\alpha h$, we get the equivalent congruence

$$4\alpha hF \equiv gd(Z^2 - \alpha^2 Nw^2 - Mv^2 + 2\alpha Pwv) \equiv 4\alpha h G(\pi), \tag{15}$$

where $Z = 2\alpha hz + \alpha jw + Av$, and N, M, P are as in (12). Since $2\alpha h$ is prime to π we may take Z, w, v as new variables in place of z, w, v. If $N = M = 0$, then $P \neq 0$ by (13), and since $2gd\alpha P$ is prime to π by (12), (15) is solvable. Otherwise with $v = 0$ or $w = 0$ according as $N \neq 0$ or $N = 0$, $M \neq 0$, (15) is solvable by Lemma 2, and hence, since $4\alpha h$ is prime to π, (14) is solvable. This completes the proof of Lemma 2A.

Then by hypothesis (11) has a solution $z', w', v', y = \eta$, where $\eta = 1$ or π, and by Lemma 2A, if $\eta = \pi$ (and trivially if $\eta = 1$) $F \equiv G(\eta)$ has a solution $z'', w'', v'', y = \eta$.

By the Chinese Remainder Theorem there exist integers z, w, v such that $z \equiv z'$, $w \equiv w'$, $v \equiv v'$ (mod p^n), and $z \equiv z''$, $w \equiv w''$, $v \equiv v''$ (mod η). Then (11) and (14) have the same solution $z, w, v, y = \eta$, and hence, since η is prime to a and therefore to p,

$$F \equiv G(p^n \eta) \tag{16}$$

* With $v = w = 0$, change h to αh in line 9, p. 174, of the reference previously quoted.

Figure 10: Page 744 from from R.S. Underwood's *On Universal Quadratic Null Forms in Five Variables* (1931).

ON UNIVERSAL QUADRATIC NULL FORMS IN FIVE VARIABLES*

BY

R. S. UNDERWOOD

INTRODUCTION

1. We shall use L. E. Dickson's result:†

THEOREM 1. *Every universal quadratic null form in three or more variables is equivalent to a form*

$$F = 2^e gaxy + gby^2 + cyz + gd\psi(z, w, \cdots) \qquad (e \geqq 0), \tag{1}$$

where g and a are odd, a is prime to d, c is prime to g, and the greatest common divisor of the coefficients of ψ *is* 1.

We investigate the case of five variables. In (1) let

$$\psi = \alpha(hz^2 + jzw + lw^2) + Azv + Bwv + Cv^2, \tag{2}$$

where

(3) 1 is the greatest common divisor of α, A, B, C and of h, j, l, and where, by an argument which carries over from Dickson's paper, h may be taken prime to any given odd integer. We take h prime to ga.

We shall assume that one of $N, M, P \neq 0$, where $N = j^2 - 4hl$, $M = A^2 - 4\alpha hC$, $P = 2hB - jA$. For if $N = M = P = 0$, then $4\alpha h\psi = (2\alpha hz + \alpha jw + Av)^2$, where either $\alpha jw + Av$ is identically zero or it may be taken as a product of a constant by a new variable w. Hence this case reduces to the problem for three or four variables.

2. We shall need the following lemmas:

LEMMA 1. *If each of the congruences*

$$F \equiv G \quad (\text{mod } 2^e), \qquad F \equiv G \quad (\text{mod } gay), \tag{4}$$

with F as in (1) *and* (2), *has a solution x, y, z, w, v such that y is odd, then* $F = G$ *is solvable.*

---

* Presented to the Society, June 13, 1931; received by the editors in December, 1930.

† *Universal quadratic forms*, these Transactions, vol. 31, No. 1, pp. 164–189. Subsequent references to the four-variable case refer to this paper.

742

Figure 11: Page 742 from from R.S. Underwood's *On Universal Quadratic Null Forms in Five Variables* (1931).

79 STAT.] PUBLIC LAW 89-236—OCT. 3, 1965 913

qualified immigrants who are the unmarried sons or daughters of citizens of the United States.

"(2) Visas shall next be made available, in a number not to exceed 20 per centum of the number specified in section 201(a)(ii), plus any Ante, p. 911. visas not required for the classes specified in paragraph (1), to qualified immigrants who are the spouses, unmarried sons or unmarried daughters of an alien lawfully admitted for permanent residence.

"(3) Visas shall next be made available, in a number not to exceed 10 per centum of the number specified in section 201(a)(ii), to qualified immigrants who are members of the professions, or who because of their exceptional ability in the sciences or the arts will substantially benefit prospectively the national economy, cultural interests, or welfare of the United States.

"(4) Visas shall next be made available, in a number not to exceed 10 per centum of the number specified in section 201(a)(ii), plus any visas not required for the classes specified in paragraphs (1) through (3), to qualified immigrants who are the married sons or the married daughters of citizens of the United States.

"(5) Visas shall next be made available, in a number not to exceed 24 per centum of the number specified in section 201(a)(ii), plus any visas not required for the classes specified in paragraphs (1) through (4), to qualified immigrants who are the brothers or sisters of citizens of the United States.

"(6) Visas shall next be made available, in a number not to exceed 10 per centum of the number specified in section 201(a)(ii), to qualified immigrants who are capable of performing specified skilled or unskilled labor, not of a temporary or seasonal nature, for which a shortage of employable and willing persons exists in the United States.

"(7) Conditional entries shall next be made available by the Attorney General, pursuant to such regulations as he may prescribe and in *Conditional entries.* a number not to exceed 6 per centum of the number specified in section 201(a)(ii), to aliens who satisfy an Immigration and Naturalization Service officer at an examination in any non-Communist or non-Communist-dominated country, (A) that (i) because of persecution or fear of persecution on account of race, religion, or political opinion they

Figure 12: Page 913 from from the *Hart-Cellar Act* (1965).

CPSC 202: Mathematical Tools for Computer Science **Oct. 27, 2020**
Fall 2020, Extra Assignment

Due: Tuesday, November 3, 2020 at 1:00 PM

Submission Instructions: On the first page of your assignment, list:

- Your Name
- Your NetID

This assignment is due on Election Day, and it is an **entirely optional, bonus half-assignment**.

For example, if there are 10 regular assignments worth 100 points each, and your scores sum to 870, you have an 87% in the Problem Sets portion of your grade (before the curve). If you complete this assignment, you will get an extra 50 points, and the Problem Sets part of your grade becomes a 92%.

There is no technical content in this assignment, and instead you will search for historical content. I have no idea whether any of this historical content exists, but it should be interesting to search for.

To receive full credit, do **one** of the following:

1. Find an English appearance of the term **Chinese remainder theorem** prior to 1929.

   In *Chinese Researches* from 1897, Wylie describes Sun Tzu's solution, but does not refer to it as the *Chinese remainder theorem*.

   In *History of the Theory of Numbers* from 1919, Dickson refers to it as the *Chinese Problem of Remainders*.

   In his 1929 paper, *The Forms* $ax^2 + by^2 + cz^2$ *Which Represent All Integers*, Dickson first refers to it as the *Chinese remainder theorem*. This is the earliest instance that I could find. Can you find one that is earlier?

   If you find one, provide a PDF of the article.

2. Find an appearance of the term **Euclid's Algorithm** or **Euclidean Algorithm** prior to 1903. It does not have to be in English, as the lingua franca of science in the 19th century was German.

   The oldest I can find is Dickson's 1903 article *Finite Fields Whose Elements are Linear Differential Expressions*. Epsteen's 1903 article *On Linear Differential Congruences* uses the phrase "An algorithm analogous to Euclid's", which is close. Dickson and Epsteen were colleagues at the University of Chicago, and these articles appear in the same journal issue, one right after the other.

   Are we all using a name coined by some University of Chicago guys in the 1900s, or is it older? If you find an older use, provide a PDF of the article. If your reference is in German (or some other language), provide both the original text, and a translation.

3. Can you find a usage of the term **Chinese Remainder Theorem** as a *proper noun* prior to 1931?

   In his 1929 paper, Dickson refers to it in common noun form as the *Chinese remainder theorem*: note the lower case 'r' and 't'. In modern literature, it has been proper-noun-ized into *Chinese Remainder Theorem*, and even gets abbreviated to *CRT*. The earliest instance I can find of this use is Underwood's article *On Universal Quadratic Null Forms in Five Variables* from 1931. Underwood was at University of Chicago, and name-checks Dickson in the first sentence of the paper.

   Is this the first use of CRT as a proper noun? If you find an earlier one, provide a PDF of the article.

4. In China, what other names are used for the **Chinese Remainder Theorem**? If you find an alternate name, provide both the original text, as well as a translation. Obviously, this problem is limited to students that can read Chinese.