MATH 4820/5820-3: 1ST–4TH WEEK SYLLABUS
2:00 – 2:50 MWF ECCR 139
AN INTRODUCTION USING CHAPTERS 1–6

PROF. MICHAEL D. FRIED, OFFICE MATH. DEPT. #223

Book: John Stillwell, Mathematics and its History, Spring 3rd Edition 2010

1. An overview to the start

1.1. **Numbers and arithmetic.** *p. xi:* We can "integrate" $\frac{1}{\sqrt{1-x^2}}$, but not $\frac{1}{\sqrt{1-x^4}}$. Later, we can "solve" $x^3+x+1=0$, but not x^5+x+1. Questions that come up: What do those two statements mean? What do we have to do to perform these actions in the first cases? Why can't we do those actions in the last cases?

p. 12: Recall that $\sqrt{2}$ is irrational. How do we use that 2 is a prime? There are two possible definitions of primes.

(1.1a) A positive integer, m, divisible only by itself and 1.
(1.1b) A positive integer for which if $m|a\cdot b$, then either $m|a$ or $m|b$.

Question 1.1. Consider the number $p=4$ and the integers $a=8$ and $b=2$. How does (1.1b) support or disallow that $p=4$ is a prime in this case?

1.2. **For what numbers n is it hard to find a factor?** Obviously, it isn't an even number, or one divisible by 3 or 5. Can we sometimes show a number factors without actually finding the factors? Do we allow using computers or not? If we do allow them, how do we test factorization?

Example 1.2. How might we easily factor 8051, a number that is approximately 90^2. Consider $90^2-8051=49=7^2$.

(1.2a) Thus, $90^2-7^2=(90-7)(90+7)$; it factors.
(1.2b) More generally,

$$4a\times b=(a+b)^2-(a-b)^2 \text{ or } a\times b=((a+b)/2)^2-((a-b)/2)^2.$$

So, when is this formula useful for factoring numbers?

1.3. **Euclidean Algorithm, p. 41–43.** What to expect from and how to calculate the least integer in $\{ax+by \mid (x,y)\in\mathbb{Z}^2\}$ and relatively prime n-tuples $(a_1,\dots,a_n)$.

Example 1.3. What is the greatest common integer in $12121=r_1$ and $16027=r_0$? What does it have to do with the following process? $12121\overline{)16027}$ $(r_1\overline{)r_0})$ to get quotient q_1 and remainder r_2. Then, compute $r_2\overline{)r_1}$ to get quotient q_2 and remainder r_3; compute $r_3\overline{)r_2}$ to get quotient q_3 and remainder r_4;...

If the answer is d, why does this mean that there are integers x and y such that $d=12121x+16027y$, and how do you find them?

Linear equations with integer solutions; p. 43: Given integers a, b, c, when can we solve the equation $ax + by = c$ for $x, y \in \mathbb{Z}$.

(1.3a) If it has solutions, then $\gcd(a, b) = d$ divides c (p. 74).
(1.3b) If the equation has one solution, what are the rest of the solutions?

Fundamental Theorem of Arithmetic: We refer to it as **FTA**. It says there is one and only one way to write every positive integer as a product of prime powers.

One notation is convenient for certain calculations. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\dots$, p_n the nth prime,.... **FTA** says, for every positive integer n there is a *unique* string of nonnegative integers $s_1, s_2, \dots$ with the following properties:

(1.4a) For k large $s_k = 0$; and
(1.4b) $n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k} \dots$.

Example of this notation: $15 = 3 \cdot 5 = 2^0 3^1 5^1 7^0 11^0 \cdots$. This notation gives a handy way to write $n \cdot m$, $\gcd(n, m)$ and $\operatorname{lcm}(n, m)$.

Example 1.4. If $n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k} \dots$ and $m = p_1^{s_1'} p_2^{s_2'} \dots p_k^{s_k'} \dots$, then

$$n \cdot m = p_1^{s_1+s_1'} p_2^{s_2+s_2'} \dots p_k^{s_k+s_k'} \dots$$

1.4. **Rational versus integral solutions.** Stillman also considers this "geometry versus arithmetic."

Pythagorian triples: p. 8, Diophantus' method: Start with the easiest solution of $x^2 + y^2 = z^2$, $P = (-1, 0)$. Now, draw a line with slope t with from $P = (x_0, y_0)$: $\frac{(y-y_0)}{(x-x_0)} = t$, and solve for (x, y), the other point of intersection with the circle, in terms of t. Here you get

$$(x, y) = (\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}); \text{ take } t = \frac{p}{q}.$$

Question 1.5. Would this work for any quadratic $ax^2 + by^2 = cz^2$?

Topics that come together through their involvement with irrational numbers.

Pell's equation; p. 44: $x^2 - Ny^2 = k$ with N squarefree.

(1.5a) Pythagoreans with $N = 2$, $k = 1$ considered

$$(x_0 - \sqrt{2}y)^u (x + \sqrt{2}y_0)^u = (x_u - \sqrt{2}y_u)(x_u + \sqrt{2}y_u); \ (x_0, y_0) \implies \infty\text{-ly many.}$$

(1.5b) Brahmagupta (1150 CE): Given solutions for k_1, k_2,

$$(x_i - \sqrt{N}y_i)(x_i + \sqrt{N}y_i) = k_i, k = 1, 2, \text{ found solutions for } k = k_1 k_2.$$

By showing the attempts of the earliest mathematicians to relate geometry to arithmetic, Stillman notes in different places a whole bunch of developments that related researchers from many different times.

Continued fractions: Take $\alpha_0 > 0$ to be a real number and form $\alpha_0 = n_0 + \alpha_1$, with $0 \le \alpha_1 < 1$. Stop if $\alpha_1 = 0$, but otherwise write $\alpha_1 = \frac{1}{1/\alpha_1} = \frac{1}{}n_1 + \alpha_2$, with α_2 satisfying the same properties as α_1.

Continue inductively to form the sequence $\{(\alpha_i, n_i)\}_{i=0}^{\infty}$, where by you use approximates to α_0 from the partial integer sequences $[n_0, n_1, \dots, n_k] = x_k$.

Lemma 1.6. *Euclid (p. 70) distinguished between the termination or not of the continued fraction as the distinction between rationality ($\alpha = \frac{p}{q}$) and rationality. Later Greek mathematicians distinguished between becoming periodic or not.*

Eudoxus (400 - 350 BCE) introduces *Dedekind cuts*: defining all real numbers from rational numbers, and with Dedekind introducing equivalence relations.

Example 1.7. Suppose $[n_0, n_1, \dots, n_k] = [n_0, t, t, \dots, t]$. What kind of number is α_0? For simplicity try the case $n_0 = t$. Then, $x_{k+1} = t + \frac{1}{x_k}$. In the limit $x = t + 1/x$, or $x^2 - tx - 1 = 0$. p. 48 Ex. 3.4.4 asks about $\sqrt{3}$.

p. 78-80: Pell's equation for $k = \{\pm 1, \pm 2, \pm 4\}$: Bhâskara II "solves" Pell's equation for all these values of k, with Lagrange (1768) proving his *cyclic process* always works, and Weil (1984) used only Bhâskara's concepts. The cyclic process is a kind of inverse to Ex. 1.7.

Then, there is the proof of Dirichlet (§25.2) that solves the case $k = 1$ for any N based on finding units in the ring of integers of $\mathbb{Q}(\sqrt{N})$.

Chinese remainder Thm., p. 72–74: This is certainly one of the most important theorems used today, and it is about solving linear equations of great generality, again from the Euclidean algorithm.

Theorem 1.8. *If $P_1, \dots, P_k$ are pairwise prime numbers, then for any integers $r_1, \dots, r_k$ with r_i and P_i prime, there is an integer $n \equiv r_i \mod P_i$, $i = 1, \dots, k$.*

The book suggests these steps, equivalent to Qin Jiushao's solution in 1247.

(1.6a) For $k = 1$, with A_1 and P_1 prime use the Euclidean algorithm to find u_1, v_1 such that $u_1 P_1 + v_1 A_1 = 1$. That is, u_1 is an inverse of $P_1 \mod A_1$.

(1.6b) Take $A_1 = \prod_{i=2}^{k} P_i$ so that $v_1 A_1 \equiv 1 \mod P_1$, but $\equiv 0 \mod P_i$, $i \neq 1$.

1.5. **Chap. 6: Polynomial Equations.** This is an unbelievably long story, recurring repeatedly in the most modern of mathematics. It led to the combination of algebra and geometry. If you have had linear algebra (§6.2) and Cramer's rule, then you have had some sophisticated modern mathematics, that is algorithmic *elimination* for determining when you can solve linear equations over a field and describing the solutions geometrically.

p. 90 suggests considering two polynomials in two variables, x and y, of degree m in y, regarding the the powers of y as unknowns, with coefficients in the field $K(x)$, of rational functions over a field K. Then, use elimination to form an equation in x about the nature of the common solutions of the two equations. There is a famous theorem here, called *Bezout's*. p. 91 Ex. 6.2.1. Ex. 6.2.2 give an example for which the statement is that if $f(x, y)$ and $g(x, y)$ have respective degree m and n you would never expect more than $m \cdot n$ solutions.

Indeed, you would expect exactly $m \cdot n$ solutions if counted with correct multiplicity, seriously taken up in §7.5, where it presses the big issue: Where to count solutions? Answer: in the complex numbers $\mathbb{C}$, not taken up until Chap. 14, where it mentions the proof of the *Fundamental Theorem of Algebra* by Gauss in 1799:

Theorem 1.9. *Every polynomial $y^n + a_1 y^{n-1} + \cdots + a_n$ has precisely n solutions, if counted with multiplicity.*

As late as the middle of the 1500's, the time of Fermat and Descartes, they didn't have the modern notation of powers or the idea of factorization of $f(y)$ as $(y-a)g(y)$ if you know one solution $y=a$.

A different question on solvability is whether solutions of a polynomial equation $f(y)=0$ can be found in terms of radicals.

(1.7a) p. 96 has exercises showing you can't "construct" $2^{\frac{1}{3}}$ from square roots of rational numbers.

(1.7b) §6.5 has Cardono's solution of the cubic by substituting $y=u+v$, and eliminating v. p. 99 has the solutions, but there seem to be six solutions.

(1.7c) A bigger problem: Even for $\deg(f(y))=3$, with 3 real solutions, Cardono's solution involves complex numbers.

Extra Comments about the Course:

(1.8a) Office Hours: Two of them after the course on Wednesday and Friday. We'll check if that suffices. Also, I expect to communicate by e-mail with you, and you can ask any question you like.

(1.8b) Grading:

- With a smaller class we can base much of the grade on participation and a project. For the project I will help you get put together in teams, and give you a list from which to select team topics.
- You each are responsible for a report on your part of the project.
- There will be a final exam, much based on what you got from listening to what your classmates presented in their project.

(1.8c) *Syllabus statements* from a document university hands out.

- Accommodation for Disabilities: If necessary, submit your accommodation letter from Disability Services to me.
- Classroom Behavior: in particular refers to my use of your name.
- Honor Code: All incidents of academic misconduct will be reported to the Honor Code (honor@colorado.edu); 303-492-5550).
- Sexual Misconduct, Discrimination, Harassment and/or Related Retaliation, refers to the Office of Institutional Equity and Compliance.
- Religious Holidays: I will adjust to the best of my ability to your religious and family related needs.

(1.8d) Website: This document, Syll1, and Syllabus Statements are at

http://www.math.uci.edu/~mfried/histofmathlist-fall18.html.

Up-dated versions, problem sets, project discussions, etc. will go there.

E-mail address: michael.fried@Colorado.edu

E-mail address: michaeldavidfried@gmail.com