18.781: WHERE TO GO FROM HERE

MINH-TÂM QUANG TRINH

1. Complements

Some book recommendations.

[S] Simon Singh, *Fermat's Enigma.* This book got tons of people in my generation interested in pure mathematics.

[CR] Richard Courant & Herbert Robbins, *What is Mathematics?* Edited by Ian Stewart. A good present for a smart high-schooler.

[AG] Avner Ash and Robert Gross. *Fearless Symmetry: Exposing the Hidden Patterns of Numbers.*

Some follow-ups to the lectures.

(1) At the end of the Week 4 notes, I have added a discussion of the structure of the group of units $(\mathbf{Z}/m\mathbf{Z})^\times$, including a sketch of the proof that $(\mathbf{Z}/p\mathbf{Z})^\times$ has a primitive root when p is prime.

(2) If you want to learn more about Conway's topograph, read his book, *The Sensual (Quadratic) Form* [C].

(3) If you want to learn more about groups, rings, and fields, keep reading in Artin's *Algebra* [A].

In the rest of today, I want to talk about finding number theory in encryption, signal analysis, and music.

2. The RSA Encryption System

Groups, rings and fields belong to the branch of math called algebra. According to Vladimir Arnold, one of the oldest applications of algebra is cryptography.

The most famous application of number theory to modern cryptography is the Rivest–Shamir–Adleman (RSA) system, covered in [St, Ch. 4]. I will only explain one instance of it, fixing some typos in Stillwell's text along the way.

RSA is called a *public-key* encryption scheme because some of the information can be made public. Anubis (A) wants to transmit secret messages to Bastet (B), expressed as large positive integers. For this, A and B need to agree upon:

(1) A very large positive integer of the form $N = pq$, where p and q are distinct prime integers. Specifically, N must be larger than, and coprime to, any message integer A will send.

(2) A positive integer e coprime to $\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$, such that A and B both know a positive integer d such that

$$ed \equiv 1 \pmod{\varphi(N)},$$

Date: May 15, 2023.

but d is difficult for others to guess.

A and B allow N and e to be *public*, but keep d *private*.

The form of m ensures that it is difficult to factor N, and hence, difficult to compute $\varphi(N)$. We need e coprime to $\varphi(N)$ to ensure that the integer d exists.

Now suppose Anubis wants to send a message integer m to Bastet, where m is smaller than and coprime to N. In the RSA system, he sends the remainder of m^e modulo N. We claim that:

Theorem 1. *To decrypt the message,* i.e.*, to recover Anubis's original integer m, it suffices for Bastet to compute the remainder of $(m^e)^d$ modulo N.*

Proof. Since $0 < m < N$, it suffices to show that $m^{ed} \equiv m \pmod{N}$. By assumption, we can write $ed = 1 + \varphi(N)k$ for some integer k. By Euler's theorem and m being coprime to N, we have $m^{\varphi(N)} \equiv 1 \pmod{N}$. Therefore

$$m^{ed} \equiv m \cdot (m^{\varphi(N)})^k \equiv m \pmod{N},$$

as needed. □

Stillwell's text explains why this is a relatively robust encryption scheme: Essentially, exponentiating can be made very fast, using repeated squaring, but factoring, calculating φ, and calculating primitive roots (*a.k.a.*, "the discrete log problem") are all relatively difficult.

In fact, the RSA encryption scheme can be generalized to any finite group G. The public data are the group G and an integer e; the private datum is an integer d such that $ed \equiv 1 \pmod{|G|}$. The messages that can be encrypted are the elements $g \in G$. Anubis sends g^e, and Bastet decrypts the message by calculating $(g^e)^d$. Lagrange's theorem, applied to the cyclic subgroup $\langle g \rangle \subseteq G$, ensures that $(g^e)^d = g$. However, this encryption scheme is only secure if it is difficult to determine d from G and e: that is, only if the discrete log problem is difficult to solve in G.

3. Discrete Signal Analysis

3.1. **Fourier Analysis.**

Fourier analysis is the study of how to decompose a signal, such as an acoustic signal, into simple constituents, such as sinusoidal waves. If $f : \mathbf{R} \to \mathbf{C}$ is a nice (*e.g.*, continuous) function that exhibits some periodicity, say, $f(x+1) = f(x)$ for all $x \in \mathbf{R}$, then there is an expansion of the form

$$f(x) = \sum_{n \in \mathbf{Z}} \hat{f}(n) e_n(x), \qquad \text{where } e_n(x) = e^{2\pi i n x}, \tag{3.1}$$

called the Fourier series of f. Above, the notation $\sum_{n \in \mathbf{Z}}$ really means the $N \to \infty$ limit of the partial sum $\sum_{-N \leq n \leq N}$. The function e_n can be viewed as the complex version of the sinusoidal wave of frequency n, and the term $\hat{f}(n)$ is called the nth *Fourier coefficient* of f.

Note that in this setup, the periodic function f carries the same information as a function $\bar{f} : \mathbf{R}/\mathbf{Z} \to \mathbf{C}$, where $\mathbf{R}/\mathbf{Z}$ denotes a quotient group with respect to addition. Similarly, the functions e_n descend to functions $\bar{e}_n : \mathbf{R}/\mathbf{Z} \to \mathbf{C}$ such that

$$\bar{e}_n(x+y) = \bar{e}_n(x) \cdot \bar{e}_n(y).$$

So we can also regard the $\bar{e}_n$ as group homomorphisms from $\mathbf{R}/\mathbf{Z}$ under addition into $\mathbf{C}^\times$ under multiplication.

There is an analogue of Fourier analysis in which we replace $\mathbf{R}/\mathbf{Z}$ with $\mathbf{Z}/m\mathbf{Z}$. For a function $\psi : \mathbf{Z}/m\mathbf{Z} \to \mathbf{C}$, the analogue of (3.1) is an expansion

$$\psi(x) = \sum_{a=0}^{m-1} \hat{\psi}(a)\varepsilon_a(x), \qquad \text{where } \varepsilon_a(x) = e^{2\pi i a x/m}.$$

Note that ε_a is well-defined because if $x \equiv y \pmod m$, then $e^{2\pi i a(x-y)/m} = 1$, whence $e^{2\pi i a x/m} = e^{2\pi i a y/m}$. The coefficients $\hat{\psi}(a)$ can be calculated using a discrete *inverse Fourier transform*:

$$\hat{\psi}(a) = \frac{1}{p}\sum_{x=0}^{m-1} \psi(x)\varepsilon_a(-x).$$

Note the outer factor of $\frac{1}{p}$ and the minus sign inside the sum.

3.2. **Autocorrelations.** In applications of signal analysis, such as the design of concert halls [T, Ch. 8], it is useful to find periodic functions f such that the *power spectrum* of values $|\hat{f}(n)|^2$ is roughly uniform in n. This problem turns out to be closely related to the study of the *autocorrelation function*

$$A_f(t) = \int_0^1 f(x+t)\overline{f(x)}\,dx.$$

Small values for A_f roughly mean that f has low interference with its phase shifts. The discrete analogue of A_f is

$$A_\psi(t) = \sum_{x \in \mathbf{Z}/m\mathbf{Z}} \psi(x+t)\overline{\psi(x)}.$$

Example 2. If ψ is constant, so that $\psi(x) = 1$ for all x, then $A_\psi(t) = m$ for all t.

Example 3. If ψ is a "spiked pulse" at 0, so that $\psi(0) = \sqrt{m}$ and $\psi(x) = 0$ for $x \not\equiv 0$, then $A_\psi(0) = m$ and $A_\psi(t) = 0$ for $t \not\equiv 0$.

Example 4. When $m = p > 2$, an odd prime, there is another solution as good as the spiked pulse. Namely, take $\psi(x) = e^{2\pi i x^2/p}$. (Note that this function is closely related to quadratic residues modulo p.) We calculate

$$A_\psi(t) = \sum_{x \in \mathbf{Z}/p\mathbf{Z}} e^{2\pi i(x+t)^2/p} \cdot e^{-2\pi i x^2/p} = e^{2\pi i t^2/p} \sum_{x \in \mathbf{Z}/p\mathbf{Z}} e^{2\pi i(2xt)/p}.$$

If $t \not\equiv 0 \pmod p$, then $2xt$ cycles through all congruence classes mod p, as we run over $x \in \mathbf{Z}/p\mathbf{Z}$. We therefore have $A_\psi(0) = p$ and $A_\psi(t) = 0$ for $t \not\equiv 0$.

Exercise 5. Show the discrete Wiener–Khintchine theorem: For any function $\psi : \mathbf{Z}/m\mathbf{Z} \to \mathbf{C}$ and value of a, we have

$$\hat{A}_\psi(a) = p|\hat{\psi}(a)|^2$$

Exercise 6. Calculate $\hat{A}_\psi$ for Examples 2–4. Then use the Wiener–Khintchine theorem to show that the power spectra $\{|\hat{\psi}(a)|^2\}_a$ are uniform in the second and third examples, but not in the first.

4. Musical Tuning

For the ancient Greeks, the first application of number theory was to music. Sounds are made by vibrating waves. The wavelength and frequency of a sound are inversely proportional to each other. Two waves sound good together iff their wavelengths, or equivalently frequencies, form a ratio that has small numerator and denominator.

The ratio $1 : 2$ corresponds to the musical interval called the octave: The higher of the two notes in an octave has twice the frequency, and half the wavelength, of the lower note. What musicians and engineers call the harmonic series is not a sum, but the sequence of ratios

$$1 : 2, \quad 2 : 3, \quad 3 : 4, \quad 4 : 5, \quad \ldots,$$

viewed as a sequence of musical intervals, starting with the octave and growing successively narrower.

On Problem Set 2, one of the questions asked you to show that $x^2 = 2y^2$ has no solutions where x, y are both positive integers. This means $\sqrt{2}$ is irrational. Why did the Greeks discover this theorem? The standard answer is the geometry of the 45°-45°-90° triangle. But I can also imagine the Greeks looking for the *ratio* of frequencies r that would bisect the octave:

$$1 : r = r : 2.$$

The irrationality of r would have provided them with a mathematical explanation for the disturbing, dissonant quality of this interval.

In the modern West, the most common tuning system is equal temperament, where an octave is divided into 12 intervals of equal frequency ratio. The fact that $\sqrt[12]{2}$ is irrational means that none of the intervals we are used to hearing, except octaves, would actually sound "in tune" to an ancient Greek.

References

[A] M. Artin. *Algebra*. 2nd Ed. Pearson (2010).

[AG] A. Ash & R. Gross. *Fearless Symmetry: Exposing the Hidden Patterns of Numbers*. Princeton University Press (2008).

[C] J. H. Conway. *The Sensual (Quadratic) Form*. Assisted by F. Y. C. Fung. *The Carus Mathematical Monographs*, Number Twenty-Six. The Mathematical Association of America (1997).

[CR] R. Courant & H. Robbins. *What is Mathematics? An Elementary Approach to Ideas and Methods*. 2nd Ed. Rev. I. Stewart. Oxford University Press (1996).

[S] S. Singh. *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem*. Walker & Co., (1998).

[St] J. Stillwell. *Elements of Number Theory*. Springer (2003).

[T] A. Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press (1999).

Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139

Email address: `mqt@mit.edu`