# MAT 302: LECTURE SUMMARY

Thus far in this course, we've discussed *symmetric* ciphers, in which Alice and Bob use the same key and (essentially) the same algorithm to encrypt and decrypt. This has been the main weakness in all of these: because both Alice and Bob require the key, it must be securely transported between the two of them at some point. This is presumably a nontrivial task, since otherwise Alice and Bob wouldn't need to use encryption in the first place!

In the 1970s, several researchers independently arrived at the idea of a different type of cryptography, known as *asymmetric* or *public key* cryptography, which solves the problem of key exchange. The underlying idea is that Bob establishes a "mailbox" into which anyone (including Alice) can easily deposit a message, but which only Bob can open to view the messages inside. To accomplish this, Bob sets up a *one-way function*, i.e. a procedure which is simple to do (and hence makes it easy for Alice to encode a message) but difficult to undo without extra information (and hence tough to decode for anyone other than Bob). We will discuss one-way functions more carefully in the next lecture, but for now we gave an example of a procedure which is simple to do but difficult to undo: factorization.

Calculating $23 \times 27 = 621$ is a triviality. However, factoring a number of comparable size (say, 623) is a very involved task. One (not so clever) approach is check divisibility by all numbers between 2 and 623, and proceed recursively. A much better approach is to just check divisibility by all the numbers between 2 and $\sqrt{623} \approx 25$. An even better approach is to check divisibility by the *primes* smaller than $\sqrt{623}$; there are only nine of these, so this is not an overwhelming task. Still, if rather than dealing with 623 we were trying to factor a 200 digit number, we'd be checking all the primes less than $10^{100}$. This is an enormous (and totally infeasible) computation. By contrast, multiplying two 100-digit numbers takes rouchgly $100^2 = 10,000$ operations, which is very doable.

This led us to a discussion of the approximating the number of primes less than $x$. A famous theorem, first conjectured by Gauss when he was 14 but not proved until more than a century later, is the following:

**Theorem 1** (The Prime Number Theorem). *Let $\pi(x)$ denote the number of primes $\leq x$. Then*

$$\pi(x) \sim \int_2^x \frac{dt}{\log t}$$

*where* $\log$ *denotes the natural logarithm.*

You may wonder why the right hand side is left as an integral. This is for a simple reason: the function $\frac{1}{\log t}$ has no antiderivative in elementary functions. Thus, the integral cannot be simplified.

*Date*: March 1st, 2011.

However, it can be approximated: integrating by parts shows that

$$\int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$$

which gives a more down-to-earth asymptotic for $\pi(x)$. However, $\frac{x}{\log x}$ is a much worse approximation to $\pi(x)$ than is the integral given in the Prime Number Theorem. This is a natural point to state one of the most notorious unsolved problems in mathematics:

**Conjecture 2** (The Riemann Hypothesis)**.** *For any $\epsilon > 0$,*

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O_\epsilon\left(x^{1/2+\epsilon}\right)$$

*where the implicit constant in the error term depends only on $\epsilon$.*

It's worth noting that if we replace the integral by $\frac{x}{\log x}$, the above approximation is false.

Before leaving the subject of counting primes, I asked for the proportion of positive integers which are prime. This is not a well-posed question, in the sense that it's not obvious exactly what the word *proportion* means: there are infinitely many positive integers, and infinitely many primes. Still, this can be precise in a way which is fairly intuitive. To illustrate the idea, what proportion of positive integers are even? The only reasonable answer is $1/2$. One way to obtain this formally is to determine the proportion of the integers $\leq x$ which are even, divide this by $x$, and let $x$ tend to infinity; in other words, the proportion of positive integers which are even should be

$$\lim_{x\to\infty} \frac{\#\{n \leq x \ : \ 2 \mid n\}}{x} = \lim_{x\to\infty} \frac{[x/2]}{x} = \lim_{x\to\infty} \frac{x/2 + O(1)}{x} = \lim_{x\to\infty} \left(\frac{1}{2} + O\left(\frac{1}{x}\right)\right) = \frac{1}{2}$$

We can do a similar calculation to determine the proportion of positive integers which are prime:

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = \lim_{x\to\infty} \frac{O\left(\frac{x}{\log x}\right)}{x} = \lim_{x\to\infty} O\left(\frac{1}{\log x}\right) = 0$$

Colloquially, this says that the primes are extremely sparse: or rather more crudely, that 0% of all positive integers are prime.

Next lecture, we will take up the topic of asymmetric cryptography in more detail, beginning with one of the classic examples of such a cipher: RSA.