Lecture-5

1 Primality tests

It is easy to see that an integer $n > 1$ is prime if and only if it is not divisible by none of the primes $p \leq \sqrt{n}$. For example, we see that 101 is prime as it is not divisible by none of the primes $p \leq \sqrt{101}$, namely, $2, 3, 5$ and 7. This method of primality-testing is effective for fairly small integers n, since there are not too many primes p to consider. But when n becomes large it is very time-consuming. There are alternative algorithms using some very sophisticated number theory which will determine primality for large integers much more efficiently.

AKS Primality test: In 2002, Manindra Agrawal, Neeraj Kayal, and Nitin Saxena from the Department of Computer Science and Engineering at IIT Kanpur invented a primality-testing algorithm which is the most efficient algorithm to date. For more details, see “PRIMES is in P, **Annals of Mathematics** 160 (2004), pp. 781–793.

[From Left to Right: Manindra Agrawal, Neeraj Kayal, and Nitin Saxena]

2 Primes in Arithmetic Progression

We have already seen that the list of primes continues without end. We know that any odd prime p is either of the form $4k + 1$ or $4k + 3$ for some integer k. The primes $3, 7, 11, 19, 23, 31, 43, 47, \ldots$ are of the form $4k + 3$, whereas the primes $5, 13, 17, 29, 37, 41, 53, 61, \ldots$ are of the form $4k + 1$. We can ask the following questions:

- Are there infinitely many primes of the form $4k+3$?
- Are there infinitely many primes of the form $4k+1$?

The answer to both the questions is yes. We can again use Euclid's idea to produce a list of infinitely many primes of the form $4k+3$. Given a finite list of primes of the form $4k+3$, it produces a new prime that isn't in the original list. More precisely, suppose that $3 < p_1 < p_2 < p_3 < \cdots < p_m$ is a list of primes each of the form $4k+3$. Consider the number $N = 4p_1p_2\cdots p_m + 3$. Since N is odd, so is each prime p dividing N, and hence p has the form $4k+1$ or $4k+3$ for some k. If each such p has the form $4k+1$, then N (being a product of such integers) must also have this form, which is false. Hence, N must be divisible by at least one prime p of the form $4k+3$. It is clear from the definition of N that none of $3, p_1, p_2, \ldots, p_m$ divides N. Thus, p is not in the original list, so we may add it to the list and repeat the process. In this way we can produce a list of primes of the form $4k+3$ that is as long as we want. This proves that there must be infinitely many primes of the form $4k+3$.

We can use the ideas in the proof to create a list of primes of the form $4k+3$. We start with the list consisting of the single prime $\{7\}$ (remember that 3 is not allowed in the list). We compute $N = 4 \times 7 + 3 = 31$, which is a prime of the form $4k+3$. So, we add this new prime to the list, and the list now becomes $\{7, 31\}$. We compute $N = 4 \times 7 \times 31 + 3 = 871$, which is not a prime and it factors as $N = 13 \times 67$. As the proof tells, at least one of the factors will be of the form $4k+3$, and in this case it is the prime 67. So, we add 67 to the list. Proceeding in this way, here is how the list grows:

$$\begin{aligned}
&\{7\}\\
&\{7, 31\}\\
&\{7, 31, 67\}\\
&\{7, 31, 67, 19\}\\
&\{7, 31, 67, 19, 179\}\\
&\{7, 31, 67, 19, 179, 197788559\}\\
&\text{etc.}
\end{aligned}$$

There are also infinitely many primes of the form $4k+1$. However, the above idea does not work for primes of the form $4k+1$. The reason is that the product of two numbers each of the form $4k+3$ is a number of the form

$4k+1$. The proof of infinitude of primes of the form $4k+1$ is a little more subtle. We will prove it later.

The numbers of the form $4k+3$ form an arithmetic progression (AP) with initial term 3 and common difference 4. A few terms of this AP are $3, 7, 11, 15, 19, 23, 27, \ldots$. We have showed that there are infinitely many terms in this AP which are prime numbers. In general, we fix two positive integers a and m, and consider the AP: $a, a+m, a+2m, a+3m, a+4m, \ldots$. We ask the question: does this AP contain infinitely many prime numbers? There is one situation in which the answer is negative, that is if a and m have a common factor greater than 1. In this case, the numbers $a+m, a+2m, a+3m, a+4m, \ldots$ are all composite. A famous theorem of Dirichlet from 1837 says that if $\gcd(a, m) = 1$, then there are infinitely many primes of the form $a + mk$.

Theorem 1 (Dirichlet's Theorem on Primes in AP)**.** *Let a and m be positive integers with $\gcd(a, m) = 1$. Then there are infinitely many primes of the form $a + mk$, where k is an integer. That is, the arithmetic progression $a, a+m, a+2m, a+3m, a+4m, a+5m, \ldots$ contains infinitely many primes.*

The proof of Dirichlet's Theorem is quite involved and it requires some advanced topics from analytic number theory.

3 Gaps between primes

Another interesting problem is to study more of the numerics regarding gaps between one prime and the next, rather than the tally of all primes. More precisely, given a real number X and a positive integer k, we define

$$\mathrm{Gap}_k(X)$$

to be the number of pairs of *consecutive* primes (p, q) with $q < X$ that have "gap k", that is, their difference $q - p$ is k. Here p and q are both primes such that $p < q$, and there are no primes between p and q. For example, $\mathrm{Gap}_2(10) = 2$, since the pairs $(3, 5)$ and $(5, 7)$ are the pairs less than 10 with gap 2, and $\mathrm{Gap}_4(10) = 0$ as there are no consecutive primes p and q (both less than 10) with gap $q - p = 4$. There is no fun at all to try to guess how many pairs of primes p, q there are with gap $q - p$ equal to a fixed odd number, since the difference of two odd numbers is even. In Table 1, we list values of $\mathrm{Gap}_k(X)$ for more values of X and k.

Table 1: Values of $\mathrm{Gap}_k(X)$

X	10	10^2	10^3	10^4	10^6	10^8
$\mathrm{Gap}_2(X)$	2	8	35	205	8169	440312
$\mathrm{Gap}_4(X)$	0	7	40	202	8143	440257
$\mathrm{Gap}_6(X)$	0	7	44	299	13549	768752
$\mathrm{Gap}_8(X)$	0	1	15	101	5569	334180
$\mathrm{Gap}_{100}(X)$	0	0	0	0	2	878

A twin prime pair is a pair of prime numbers (p, q) with gap 2. For example, $(3, 5), (5, 7), (41, 43)$ are twin prime pairs. From Table 1, we have $\mathrm{Gap}_2(100) = 8$, and the eight such twin prime pairs are

$$(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73).$$

People have used computers to compute long list of twin primes. As of December 2022, the largest known twin primes are

$$2996863034895 \cdot 2^{1290000} - 1 \quad \text{and} \quad 2996863034895 \cdot 2^{1290000} + 1.$$

Conjecture 1 (The Twin Primes Conjecture)**.** *There are infinitely many primes p so that $p + 2$ is also prime. That is,*

$$\lim_{X\to\infty} \mathrm{Gap}_2(X) = \infty.$$

Twin primes have been studied extensively, and a more general conjecture was posed, stating that all even gaps between prime numbers occur infinitely often, that is, for every even k, $\lim\limits_{X\to\infty} \mathrm{Gap}_k(X) = \infty$. There is not much progress in proving these conjectures.

On April 17, 2013, Yitang Zhang announced a proof that for some integer N that is less than 70 million, there are infinitely many pairs of primes that differ by N. The results of Zhang as sharpened by James Maynard (and others) tell us that for at least one even number k among the even numbers $k \leq 246$, $\mathrm{Gap}_k(X)$ goes to infinity as X goes to infinity, that is, there are infinitely many pairs of primes that differ by k for some even $k \leq 246$. This huge discovery, coupled with an ongoing Polymath project, may one day uncover the proof of the Twin Primes Conjecture, or we may need to find a completely new way of analysing this unsolved mystery to finally tame

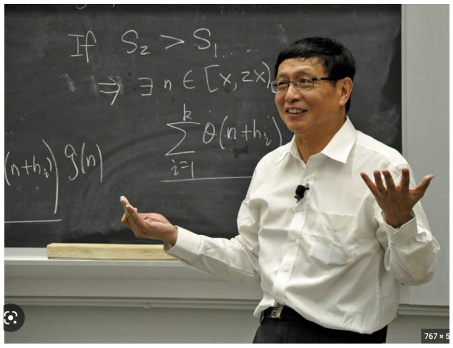
If $S_2 > S_1$
$\Rightarrow \exists n \in [x, 2x)$
$\sum_{i=1}^{k} \theta(n+h_i)$
$(n+h_i)) g(n)$
767 × 5

Figure 1: Yitang Zhang

Figure 2: James Maynard

this problem. Maynard was awarded the Fields Medal 2022 for “contributions to analytic number theory, which have led to major advances in the understanding of the structure of prime numbers”.