18.785: Analytic Number Theory, MIT, spring 2007 (K.S. Kedlaya)
The Bombieri-Vinogradov theorem (statement)

In this unit, we state the Bombieri-Vinogradov theorem, which is a surprisingly strong control on the error terms in the prime number theorem in arithmetic progressions. We also mention some related theorems and conjectures. To attack these (which we will do in the next unit), we will need to bring to bear everything we have studied in the course so far!

1 Statement of the theorem

For m, N coprime positive integers, put

$$\psi(x; N, m) = \sum_{n \leq x, n \equiv m \pmod{N}} \Lambda(n).$$

Recall that the prime number theorem in arithmetic progressions says $\psi(x; N, m) \sim x/\phi(N)$, and that unconditionally we could get an error term

$$\psi(x; N, m) = \frac{x}{\phi(N)} + O(x(\log x)^{-A})$$

for any fixed $A > 0$. This is only meaningful if $N = O((\log x)^A)$. However, under GRH (for the Dirichlet characters of modulus N),

$$\psi(x; N, m) = \frac{x}{\phi(N)} + O(x^{1/2}(\log x)^2),$$

and this is meaningful for $N = O(x^{1/2}(\log x)^{-2})$.

The Bombieri-Vinogradov theorem is an amazingly strong unconditional replacement for the GRH bound. It says that if you pick out the worst error term modulo N for *each* N up to about $x^{1/2}$, and add these up, you get roughly what GRH predicts you should get.

Theorem 1 (Bombieri-Vinogradov). *For any fixed $A > 0$, there exist constants $c = c(A)$ and $B = B(A)$ such that*

$$\sum_{N \leq Q} \max_{m \in (\mathbb{Z}/N\mathbb{Z})^*} \left| \psi(x; N, m) - \frac{x}{\phi(N)} \right| \leq cx(\log x)^{-A}$$

for $Q = x^{1/2}(\log x)^{-B}$.

It is expected that one can do better than this.

Conjecture 2 (Elliott-Halberstam). *For any fixed $A > 0$ and $\epsilon > 0$, there exists $c > 0$ such that*

$$\sum_{N \leq Q} \max_{m \in (\mathbb{Z}/N\mathbb{Z})^*} \left| \psi(x; N, m) - \frac{x}{\phi(N)} \right| \leq cx(\log x)^{-A}$$

for $Q = x^{1-\epsilon}$.

This conjecture appears to be extremely hard; for instance, it is not known to follow from GRH. One of the results of Goldston-Pintz-Yıldırım is that the Elliott-Halberstam almost implies the twin primes conjecture: it implies that there are infinitely many pairs of primes at distance ≤ 16. In fact, this (with 16 replaced by some other constant, depending on ϵ) would follow if we could prove the weaker version of Elliott-Halberstam in which $Q = x^{1/2+\epsilon}$, for any fixed $\epsilon > 0$. (Even that does not follow from GRH.)

Note that in the Bombieri-Vinogradov theorem, for each modulus N we look at the worst error term among arithmetic progressions of that modulus. If we instead average over the progressions, we should be able to take Q larger, and in fact that is what happens. (Note: there is a typo in the statement of the theorem in Iwaniec-Kowalski.)

Theorem 3 (Barban, Davenport, Halberstam)**.** *For any fixed $A > 0$, there exist constants $c = c(A)$ and $B = B(A)$ such that*

$$\sum_{N \leq Q} \sum_{m \in (\mathbb{Z}/N\mathbb{Z})^*} \left(\psi(x; N, m) - \frac{x}{\phi(N)} \right)^2 \leq cx^2 (\log x)^{-A}$$

for $Q = x(\log x)^{-B}$.

Finally, we note that Bombieri proved a slightly stronger result, which I will not be proving in this course. (See Davenport §28 for a proof by Montgomery.)

Theorem 4. *For any fixed $A > 0$, there exists $c > 0$ such that*

$$\sum_{N \leq Q} \max_{m \in (\mathbb{Z}/N\mathbb{Z})^*} \left| \psi(x; N, m) - \frac{x}{\phi(N)} \right| \leq cx^{1/2} Q (\log x)^5$$

for $x^{1/2}(\log x)^{-A} \leq Q \leq x^{1/2}$.

Exercises

1. (a) Check that Theorem 4 implies Theorem 1.

   (b) Check that Conjecture 2 implies a slightly weakened version of Theorem 3, in which we take $Q = x^{1-\epsilon}$.

2. Use the Bombieri-Vinogradov theorem, plus the strong Brun-Titchmarsh inequality

   $$\pi(x + y; N, m) - \pi(x; N, m) < \frac{2y}{\phi(N) \log(y/N)} + O\left(\frac{y}{N \log^2(y/N)} \right)$$

   (where $\pi(x; N, m)$ is the number of primes $p \leq x$ with $p \equiv m \pmod{N}$) to prove that

   $$\sum_{p \leq x} \tau(p - 1) \sim \frac{\zeta(2)\zeta(3)}{\zeta(6)} x,$$

   where $\tau(n)$ counts the number of divisors of n. (Hint: use Dirichlet's hyperbola method to reduce to counting primes $\equiv 1 \pmod{d}$ over $d \leq \sqrt{x}$.)