18.785: Analytic Number Theory, MIT, spring 2007 (K.S. Kedlaya)
The Bombieri-Vinogradov theorem (proof) (revised 9 May 07)

In this unit, we prove the Bombieri-Vinogradov theorem, in the form stated in the previous unit.

1 Bounding character sums

For f an arithmetic function, put

$$D_f(x; N, m) = \sum_{n \leq x, n \equiv m \pmod{N}} f(n) - \frac{1}{\phi(N)} \sum_{n \leq x, n \in (\mathbb{Z}/N\mathbb{Z})^*} f(n);$$

that is, $D_f(x; N, m)$ measures the deviation between the sum of f on an arithmetic progression, and the sum on all arithmetic progressions of the same modulus. The following lemma tells us that bounding this deviation allows us to control the sum of f twisted by a Dirichlet character.

Lemma 1. *Let f be an arithmetic function with support in $\{1, \dots, x\}$, and put $|f|_2 = (\sum_n |f(n)|^2)^{1/2}$. Suppose that for some $\Delta \in (0, 1]$, we have*

$$|D_f(x; N, m)| \leq x^{1/2} \Delta^9 |f|_2 \tag{1}$$

whenever $m \in (\mathbb{Z}/N\mathbb{Z})^*$. Then for any nonprincipal character χ of modulus r, and any positive integer s,

$$\left| \sum_{n \in (\mathbb{Z}/s\mathbb{Z})^*} f(n)\chi(n) \right| \leq x^{1/2} \Delta^3 r \tau(s) |f|_2.$$

Proof. By Möbius inversion, we can write

$$\sum_{n \in (\mathbb{Z}/s\mathbb{Z})^*} f(n)\chi(n) = \sum_{k|s} \mu(k) \sum_{n \equiv 0\,(k)} f(n)\chi(n).$$

We split this sum on k at $K = \Delta^{-6}$. We bound the sum for each fixed $k > K$ by Cauchy-Schwarz; the total is thus dominated by

$$\sum_{k|s, k>K} |f|_2 (x/k)^{1/2} \leq |f|_2 x^{1/2} K^{-1/2} \tau(s).$$

For the terms $k \leq K$, we write the sum as (using Möbius inversion again)

$$\sum_{k|s, k \leq K} \mu(k) \sum_{\ell | k} \mu(\ell) \sum_{n \in (\mathbb{Z}/\ell\mathbb{Z})^*} f(n)\chi(n).$$

We split the inside sum over classes modulo ℓr; on each class, we apply (1). Since we are summing over all residue classes, and χ is nonprincipal, the main terms cancel out; the sum is thus dominated by

$$|f|x^{1/2}\Delta^9 \sum_{k|s,k\le K} \sum_{\ell|k} |\mu(\ell)|\phi(\ell r) \le |f|_2 x^{1/2}\Delta^9 K\phi(r)\tau(s).$$

Since $K = \Delta^{-6}$, we may add the two bounds to give the desired inequality. $\square$

Using the large sieve inequality, we obtain the following.

Theorem 2. *There exists an absolute constant $c > 0$ with the following property. Let f be an arithmetic function with support in $\{1, \dots, x\}$ satisfying (1). Let g be an arithmetic function with support in $\{1, \dots, y\}$, and let $h = f \star g$ be the Dirichlet convolution. Then*

$$\sum_{N\le Q} \max_{m\in(\mathbb{Z}/N\mathbb{Z})^*} |D_h(xy; N, m)| \le c|f|_2|g|_2(\Delta(xy)^{1/2} + x^{1/2} + y^{1/2} + Q)\log^2 Q.$$

Proof. We have

$$D_h(xy; N, a) = \frac{1}{\phi(N)} \sum_{\chi\ne\chi_0} \overline{\chi}(a) \left(\sum_m f(m)\chi(m)\right) \left(\sum_n g(n)\chi(n)\right),$$

with χ running over Dirichlet characters of modulus N. Rewriting this as a sum only over primitive characters (factoring $N = rs$, where r is the "primitive modulus"), and using the fact that $\phi(rs) \ge \phi(r)\phi(s)$ for all r, s, we can bound the left side of the desired inequality by

$$\sum_{s\le Q} \frac{1}{\phi(s)} \sum_{1<r\le Q} \frac{1}{\phi(r)} \sum_\chi \left|\sum_{(m,s)=1} f(m)\chi(m)\right| \left|\sum_{(n,s)=1} g(n)\chi(n)\right|, \tag{2}$$

with χ now running over primitive characters of level r.

We now split the sum over r at $R = \Delta^{-1}$. For $r \le R$, we apply Lemma 1; those terms are dominated by

$$|f||g|y^{1/2}\Delta^3 \sum_{s\le Q} \frac{\tau(s)}{\phi(s)} \sum_{r\le R} r \le c|f||g|y^{1/2}\Delta^3 R^2 \log^2 Q.$$

(Note: we are not doing anything to the g terms other than bounding the whole sum by $|g|$ and pulling it out. We apply the lemma to the f terms.) For $r > R$, we split the sum further into ranges like $P < r \le 2P$ and apply the multiplicative large sieve inequality in each range. Rather, we apply it twice: once with the f sum to obtain

$$\sum_{P<r\le 2P} \frac{1}{\phi(r)} \sum_\chi \left|\sum_{(m,s)=1} f(m)\chi(m)\right|^2 \le \frac{1}{P}(4P^2 + x - 1)|f|_2^2,$$

and again with the g sum. Putting together with Cauchy-Schwarz, we get a bound

$$\sum_{P<r\leq 2P} \frac{1}{\phi(r)} \sum_{\chi} \left| \sum_{m\in(\mathbb{Z}/s\mathbb{Z})^*} f(m)\chi(m) \right| \left| \sum_{n\in(\mathbb{Z}/s\mathbb{Z})^*} g(n)\chi(n) \right| \leq \frac{1}{P}(4P^2+x)^{1/2}(4P^2+y)^{1/2}|f|_2|g|_2.$$

Now summing, over $P = R, 2R, \ldots$ until $P > Q$, we get a bound on the sum over r in (2) of

$$c|f|_2|g|_2(Q + x^{1/2} + y^{1/2} + x^{1/2}y^{1/2}R^{-1}).$$

(That R^{-1} is the reason we had to limit this argument to r large.) The sum over s throws on another two factors of $\log Q$, yielding the claim. □

2 Proof of the theorem

We now proceed to the proof of the Bombieri-Vinogradov theorem. First, we mention an identity of Vaughan that will be useful: for any $y, z \geq 1$ and $n > z$,

$$\Lambda(n) = \sum_{b\leq y, b|n} \mu(b) \log \frac{n}{b} - \sum_{b\leq y, c\leq z, bc|n} \mu(b)\Lambda(c) + \sum_{b>y, c>z, bc|n} \mu(b)\Lambda(c). \tag{3}$$

Given x, define the incomplete logarithm

$$\lambda(\ell) = \log \ell - \sum_{k\leq x^{1/5}, k|\ell} \Lambda(k);$$

then (3) with $y = z = x^{1/5}$ implies that for $x^{1/5} < n \leq x$,

$$\Lambda(n) = \sum_{\ell m=n, m\leq x^{1/5}} \lambda(\ell)\mu(m) + \sum_{\ell m=n, x^{1/5}<m\leq x^{4/5}} \lambda(\ell)\mu(m). \tag{4}$$

Let $\Lambda_0(n)$ and $\Lambda_1(n)$ denote the two sums on the right side of (4). Then

$$D_\Lambda(x; N, m) = D_{\Lambda_0}(x; N, m) + D_{\Lambda_1}(x; N, m) + O(x^{1/5} \log x),$$

with the error term coming from terms with $n < x^{1/5}$.

It is straightforward to prove that

$$\sum_{N\leq Q} \max_{m\in(\mathbb{Z}/N\mathbb{Z})^*} |D_{\Lambda_0}(x; N, m)| = O(Qx^{2/5} \log x), \tag{5}$$

so we concentrate on the contribution from Λ_1. We want to apply Theorem 2, but we cannot write the sum $\Lambda_1(n)$ as a convolution because of the restriction $n \leq x$.

To get around this, we cut the interval $1 \leq n \leq x$ into $O(\delta^{-1})$ subintervals of the form $y < n \leq (1 + \delta)y$, where $x^{1/5} < \delta \leq 1$ is a parameter we will set later. We cover the summation range

$$\ell m = n, x^{1/5} < m \leq x$$

by ranges

$$\ell m = n, L < \ell \leq (1+\delta)L, M < m \leq (1+\delta)M$$

with L, M taking values $(1+\delta)^j$. We run L, M over the ranges $x^{1/5} < L, M < x^{4/5}$ with $LM = x$; the only trouble is that we do not properly cover the areas $n < x^{1/5}$ and $(1+\delta)^{-1}x < n < (1+\delta)x$. The contribution from the error regions is $O(\delta N^{-1} x \log x)$.

What remains is the sum over L, M of

$$D(L, M; N, m) = \sum_{l, m \equiv m \pmod{N}} \lambda(\ell)\mu(m) - \frac{1}{\phi(N)} \sum_{lm \in (\mathbb{Z}/N\mathbb{Z})^*},$$

where l, m run over $L < \ell \leq (1+\delta)L, M < m \leq (1+\delta)M$. For each L, M, we may apply Theorem 2 with $\Delta = (\log x)^{-A}$; the hypothesis (1) is satisfied by the Siegel-Walfisz theorem (the error bound on the prime number theorem in arithmetic progressions). If we take $Q = \Delta x^{1/2}$, we get

$$\sum_{N \leq Q} \max_{m \in (\mathbb{Z}/N\mathbb{Z})^*} |D(L, M; N, m)| = O(\delta \Delta x (\log x)^3).$$

Summing over L, M, we obtain

$$\sum_{N \leq Q} \max_{m \in (\mathbb{Z}/N\mathbb{Z})^*} |D_{\Lambda_1}(x; N, m)| = O((\delta^{-1}x + \Delta)x(\log x)^3.$$

We now choose $\delta = \Delta^{1/2}$, so this bound becomes $\Delta^{1/2} x (\log x)^3$. Adding back in (5) gives

$$\sum_{N \leq \Delta x^{1/2}} \max_{m \in (\mathbb{Z}/N\mathbb{Z})^*} \left| \psi(x; N, m) - \frac{\psi(x)}{\phi(N)} \right| = O(\Delta^{1/2} x (\log x)^3).$$

Using the prime number theorem with error term, we can take $\psi(x) = x + O(\delta x)$. This gives the Bombieri-Vinogradov theorem with $B(A) = 2A + 6$.

3 The Barban-Davenport-Halberstam theorem

We leave the proof of the Barban-Davenport-Halberstam theorem to the reader; it is actually somewhat simpler than Bombieri-Vinogradov. Here is the key step.

Theorem 3. *There exists an absolute constant $c > 0$ with the following property. Let f be an arithmetic function with support in $\{1, \ldots, x\}$ satisfying* (1)*. Then*

$$\sum_{N \leq Q} \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^*} |D_f(x; N, m)|^2 \leq c|f|^2(\Delta x + Q)(\log Q)^2.$$

We note in passing the following corollary.

Corollary 4. *With conditions as in Theorem 2, for $ab \neq 0$, we have*

$$\sum_{N \leq Q, (ab,N)=1} \left| \sum_{m,n: am \equiv bn\ (N), (mn,N)=1} f(m)g(n) - \frac{1}{\phi(N)} \left(\sum_{(m,N)=1} f(m) \right) \left(\sum_{(n,N)=1} g(n) \right) \right|$$
$$\leq c|f||g|(x+Q)^{1/2}(\Delta y + Q)^{1/2} \log^2 Q.$$

Exercises

1. Prove (3).
2. Use (3) to deduce (4).
3. Prove (5).
4. Prove Theorem 3, by imitating the proof of Theorem 2.
5. Deduce Corollary 4 from Theorem 3. (Hint: rewrite the difference in terms of D_f and D_g.)