The Bombieri-Vinogradov Theorem

Giovanni Tognolini

University of Trento

July, 2022

Index

What can we say about the distribution of primes?

$$\pi(x) := \sum_{p \leq x} 1$$

Mathematicians tried to study the asymptotic behaviour of this function.

Prime Number Theorem

$$\pi(x) \approx \frac{x}{\log x}$$

What can we say about the distribution of primes in arithmetic progression?

$$\pi(x; a, q) := \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} 1$$

Mathematicians tried to study the asymptotic behaviour of this function.

Dirichlet Theorem

$$\lim_{x \to \infty} \pi(x; a, q) = \infty \iff (a, q) = 1$$

From now on we consider a, q s.t. $(a, q) = 1$.

We would like to do more

$$\pi(x; a, q) = \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} 1$$

- There are $\phi(q)$ elements coprime with q.
- We expect that primes equally distributes in each of the $\phi(q)$ congruence classes.

Ideally:

$$\pi(x; a, q) \approx \frac{\pi(x)}{\varphi(q)}$$

PNT for arithmetic progressions

$$\pi(x; a, q) \approx \frac{\pi(x)}{\varphi(q)} \approx \frac{x}{\log x} \cdot \frac{1}{\varphi(q)}$$

What about the error term?

Clearly:

$$\pi(x; a, q) = \frac{x}{\log x \cdot \varphi(q)} + o\left(\frac{x}{\log x}\right)$$

But we would like to have a more precise estimate.

This is the starting point of the Bombieri-Vinogradov theorem.
Before stating the BV theorem, we rewrite π in a different way (less intuitive, but more usable).

Replacing π with θ

$$\theta(x; a, q) := \sum_{\substack{p \le x \\ p \equiv a \bmod q}} \log p$$

$$\begin{cases} \pi(x; a, q) = \frac{\theta(x; a, q)}{\log x} + \int_2^x \frac{\theta(t; a, q)}{t(\log t)} \, dt \\ \theta(x; a, q) = \pi(x; a, q) \log x - \int_2^x \frac{\pi(t; a, q)}{t} \, dt \end{cases}$$

So that we can work with θ and then convert any estimate into an estimate for π, and vice-versa.

However, θ is still not the most convenient form to work with.

Replacing θ with ψ

$$\psi(x; a, q) := \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \Lambda(n)$$
$$= \sum_{\substack{p^k \leq x \\ p^k \equiv a \bmod q}} \log p$$

Observation

$$\psi(x; a, q) - \theta(x; a, q) \in O(x^{\frac{1}{2}} (\log x)^2)$$

In a nutshell

$$\pi \longleftarrow \theta \xleftarrow{O(x^{\frac{1}{2}}(\log x)^2)} \psi$$

What can we say about ψ?

Observation

If we assume GRH

$$\psi(x; a, q) = \frac{x}{\varphi(q)} + O(x^{\frac{1}{2}}(\log x)^2)$$

Equivalently:

$$\psi(x; a, q) - \frac{x}{\varphi(q)} \in O(x^{\frac{1}{2}}(\log x)^2)$$

We can consider

$$\Delta(x; q) := \max_{(a,q)=1} \sup_{y \leq x} \left| \psi(y; a, q) - \frac{y}{\varphi(q)} \right|$$

This object represent the maximum possible error for any congruence class modulo q for numbers $\leq x$.

$$\downarrow$$

$$\sum_{q \leq Q} \Delta(x; q) \in O(x^{\frac{1}{2}} Q) \qquad \text{(barring logarithms)}$$

What can we say
without assuming GRH?

The strongest known result for
an individual pair a and q is the following:

Theorem (Siegel-Walfisz)

Fix a real number $A > 0$. If $(a, q) = 1$ and $q \leq (\log x)^A$, we have

$$\psi(x; q, a) - \frac{x}{\varphi(q)} \in O_A(x \exp(-c\sqrt{\log x}))$$

So that:

$$\sum_{q \leq Q} \Delta(x; q) \in O(Qx \exp(-c\sqrt{\log x}))$$

Still worse than our previous estimate with GRH.

Another estimate

$$\Delta(x;q) := \max_{(a,q)=1} \sup_{y\le x} \left| \psi(y;a,q) - \frac{y}{\varphi(q)} \right|$$
$$\le \max_{(a,q)=1} \sup_{y\le x} \left\{ \left|\psi(y;a,q)\right|, \left|\frac{y}{\varphi(q)}\right| \right\}$$
$$\le \max_{(a,q)=1} \left\{ \left|\psi(x;a,q)\right|, \left|\frac{x}{\varphi(q)}\right| \right\} \le (\star)$$

Observation

$$\psi(x;a,q) = \sum_{\substack{n\le x \\ n\equiv a \bmod q}} \Lambda(n) \le (\frac{x}{q}+1)\log x \approx \frac{x\log x}{q}$$

$$\varphi(q) \gg \frac{q}{\log(q+1)} \implies \frac{x}{\varphi(q)} \ll \frac{x\log(q+1)}{q} \ll \frac{x\log x}{q}$$

$$(\star) \ll \frac{x \log x}{q}$$

So that

$$\sum_{q \leq Q} \Delta(x; q) \ll \sum_{q \leq Q} \frac{x \log x}{q}$$
$$\ll x(\log x)(\log Q)$$
$$\ll x(\log x)^2$$

Results comparison

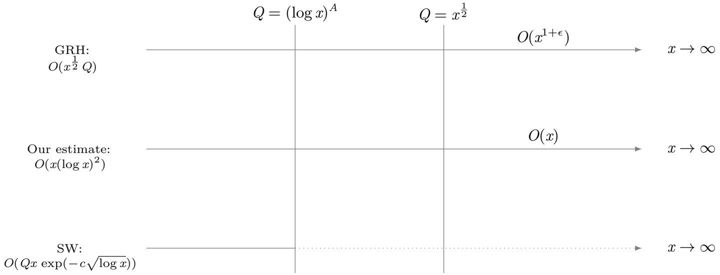

Figure: Asymptotic growth of $\sum_{q \leq Q} \Delta(x; q)$.

The more interesting case is given by $Q \leq x^{\frac{1}{2}}$.

The main theorem

Theorem (Bombieri-Vinogradov)

Fix $A > 0$. For all $x \geq 2$ and all $Q \in [x^{\frac{1}{2}}(\log x)^{-A}, x^{\frac{1}{2}}]$, we have

$$\sum_{q \leq Q} \Delta(x; q) \ll x^{\frac{1}{2}} Q (\log x)^5$$

where the absolute constant depends only on A.

A useful tool: Dirichlet characters

Definition

A Dirichlet character (of period q) is a function $\chi : \mathbb{Z} \to \mathbb{C}$ which is:

1. periodic modulo q;
2. totally multiplicative ($\chi(nm) = \chi(n)\chi(m)$);
3. satisfies $\chi(1) = 1$;
4. satisfies $\chi(n) = 0$ whenever $(n, q) \neq 1$.

Example (Principal character modulo q)

$$\chi_0(n) := \begin{cases} 1 & \text{if } (n, q) = 1 \\ 0 & \text{otherwise} \end{cases}$$

So that, if $q = 10$, the result is

n	0	1	2	3	4	5	6	7	8	9
$\chi_0(n)$	0	1	0	1	0	0	0	1	0	1

Dirichlet characters $\pmod 2$

n	0	1
$\chi_1(n)$	0	1

Dirichlet characters $\pmod 3$

n	0	1	2
$\chi_0(n)$	0	1	1
$\chi_1(n)$	0	1	-1

Observation

$$\#\{\chi \bmod q\} = \varphi(q)$$

Two types of characters: primitive and imprimitive

Suppose we have a Dirichlet character mod 5

n	0	1	2	3	4
$\chi_1(n)$	0	1	i	$-i$	1

We would like to build a new character mod $(2 \cdot 5)$ starting from χ_1

n	0	1	2	3	4	5	6	7	8	9
$\chi_2(n)$	0		0		0	0	0		0	

Now we fill the remaining values:

n	0	1	2	3	4	5	6	7	8	9
$\chi_2(n)$	0	1	0	$-i$	0	0	0	i	0	1

Formally: $\chi_2(n) = \chi_1(n)\chi_0(n)$.

Observation

Maps build up in this way are indeed characters.

Why are we making this distinction?

- Every imprimitive character is induced by a unique primitive character with a smaller period.
- Lots of estimates in number theory involve primitive characters.

$$\downarrow$$

We will convert sums over characters into sums over primitive characters, and try to estimate these objects.

One last object...

Definition (The twisted-psi function)

$$\psi(x;\chi) = \sum_{n\leq x} \chi(n)\Lambda(n)$$

...which connects characters and primes

Proposition

$$\psi(x;a,q) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)}\psi(x;\chi)$$

Another advantage...

Theorem (Sieleg-Walfisz variant)

- $A > 0$;
- $q \leq (\log x)^A$;
- χ Dirichlet character modulo q.

Then:

$$\psi(x;\chi) - \delta(\chi)x \ll_A x\exp(-c\sqrt{\log x})$$

The Bombieri-Vinogradov theorem

$$\sum_{q\leq Q} \Delta(x;q) \ll x^{\frac{1}{2}}\, Q(\log x)^5$$

We have to bound the following expression:

$$\sum_{q\leq Q}\Delta(x;q)=\sum_{q\leq Q}\max_{(a,q)=1}\sup_{y\leq x}\left|\psi(y;a,q)-\frac{y}{\varphi(q)}\right|=(\star)$$

Observation

$$\psi(y;a,q)=\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\overline{\chi(a)}\cdot\psi(y;\chi) \qquad \text{if } (a,q)=1$$

$$y=y\cdot\sum_{\chi \bmod q}\delta(\chi)=y\sum_{\chi \bmod q}\overline{\chi(a)}\delta(\chi)=\sum_{\chi \bmod q}\overline{\chi(a)}\delta(\chi)y$$

$$\left|\psi(y;a,q)-\frac{y}{\varphi(q)}\right|=\frac{1}{\varphi(q)}\cdot\left|\sum_{\chi \bmod q}\overline{\chi(a)}\psi(y,\chi)-\overline{\chi(a)}\delta(\chi)y\right|$$

$$\leq\frac{1}{\varphi(q)}\sum_{\chi \bmod q}|\psi(y,\chi)-\delta(\chi)y|$$

(7)

$$(\star) \le \sum_{q \le Q} \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \sup_{y \le x} |\psi(y, \chi) - \delta(\chi) y| = (\star\star)$$

Now we would like to apply the following estimate.

Theorem (Basic Mean Value Theorem)

Let

$$T(x, Q) := \sum_{q \le Q} \frac{q}{\varphi(q)} \sum_{\chi^* \bmod q} \sup_{y \le x} |\psi(y; \chi^*)|$$

Then

$$T(x, Q) \ll \left(x + x^{\frac{5}{6}} Q + x^{\frac{1}{2}} Q^2 \right) (\log xQ)^4$$

Problems

- sums over different characters;
- sup over different functions;
- ...

First we try to reduce our estimate to a sum over primitive characters

How to do it?

We have an arbitrary character χ mod q, and we know that for some $q^*|q$ there is a primitive character χ^* mod q^* which induces χ.

$$\downarrow$$

We would want to believe that $\psi(y;\chi)$ and $\psi(y;\chi^*)$ must be close.

$$\downarrow$$

In this way we can sum on primitive characters and pay this exchange with a (hopefully) acceptable error.

Proposition

$$\psi(y;\chi) - \psi(y,\chi^*) \in O\big((\log y)(\log q)\big)$$

(5)

$$
\begin{aligned}
(\star\star) &= \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\sup_{y\le x}|\psi(y,\chi)-\delta(\chi)y| \\
&= \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{q^*\,|\,q}\sum_{\chi^* \bmod q^*}\left(\sup_{y\le x}|\psi(y,\chi^*)-\delta(\chi^*)y| + O(\log q\cdot\log x)\right) \\
&\le \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{q^*\,|\,q}\sum_{\chi^* \bmod q^*}\left(\sup_{y\le x}|\psi(y,\chi^*)-\delta(\chi^*)y|\right)+ \\
&\quad + \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{q^*\,|\,q}\sum_{\chi^* \bmod q^*}\left(O(\log q\cdot\log x)\right)
\end{aligned}
$$

Observation

The second term is $O(Q\cdot(\log x)^2)$, and can be pulled out, and we are left to work with the first sum only.

The first sum is

$$\sum_{q \le Q} \frac{1}{\varphi(q)} \sum_{q^* \mid q} \sum_{\chi^* \bmod q^*} \sup_{y \le x} |\psi(y, \chi^*) - \delta(\chi^*) y|$$
$$\le (\text{... standard estimates ...})$$
$$\le \sum_{q \le Q} \frac{\log Q}{\varphi(q)} \sum_{\chi^* \bmod q} \sup_{y \le x} |\psi(y, \chi^*) - \delta(\chi^*) y|$$

Theorem (Siegel-Walfisz variant)

Suppose that $A > 0$ is a fixed real number. When $q < (\log x)^A$ and χ is a Dirichlet character modulo q, we have

$$\psi(x; \chi) - \delta(\chi) x \ll_A x \cdot \exp(-c(\sqrt{\log x}))$$

where c is an absolute positive constant

$\downarrow$

We can try to split the above summation.

(3)

$$\sum_{q<(\log x)^A} \frac{\log Q}{\varphi(q)} \sum_{\chi^* \bmod q} \sup_{y \le x} |\psi(y,\chi^*) - \delta(\chi^*)y| \ll (\log x)(\log x)^A x \, \exp(-c(\sqrt{\log x}))$$

$$\ll \text{ estimates with } Q \ge x^{\frac{1}{2}} (\log x)^{-A}$$

$$\ll x^{\frac{1}{2}} Q (\log x)^5$$

Now we have to deal with the remaining sum

$$\sum_{(\log x)^A \le q \le Q} \frac{\log Q}{\varphi(q)} \sum_{\chi^* \bmod q} \sup_{y \le x} |\psi(y,\chi^*) - \delta(\chi^*)y|$$

Observation

In this sum q is always greater than 2.
$\Longrightarrow$ Every primitive character χ^* modulo q is non-principal.
$\Longrightarrow \delta(\chi^*) = 0$.

It remains thus to deal with

$$\sum_{(\log x)^A \leq q \leq Q} \frac{\log Q}{\varphi(q)} \sum_{\chi^* \bmod q} \sup_{y \leq x} |\psi(y, \chi^*)| = (*)$$

Our aim (BMVT term)

$$T(x, Q) := \sum_{q \leq Q} \frac{q}{\varphi(q)} \sum_{\chi^* \mod q} \sup_{y \leq x} |\psi(y; \chi^*)|$$

We are almost done, we just have to

- get rid of the $\log Q$ factor;
- have a q factor inside the sum;
- adapt the sum.

Without going too technical

- Apply the previous modification;
- use some easy estimates and some known results in number theory;
- apply the BMVT theorem;

$$(*) \ll x^{\frac{1}{2}}\, Q(\log x)^5$$

(0)

Bombieri statement

↓

BMVT
Siegel-Walfisz
Partial Summation
...

↓

Bombieri theorem

Why?

We used without proof the BMVT (quite technical proof).

Among technical results, the proof involves a particular tool (the large sieve), which is useful in many other fields in number theory.

$\downarrow$

Makes more sense to talk about the large sieve.

What is a large sieve inequality?

- $N, M, Q \in \mathbb{N}$;
- $(a_n)_n$ sequence of real numbers;
- $S(\alpha) := \sum_{n=M+1}^{N+M} a_n e(n\alpha)$

Then we would like to have a function $\lambda(N, Q)$ s.t.

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 \leq \lambda(N, Q) \sum_{n=M+1}^{N+M} |a_n|^2$$

An inequality of this form is called a "*large sieve inequality*".

Observation

There is at least a function $\lambda(N, Q)$ which satisfies

$$\sum_{q\leq Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left|S\left(\frac{a}{q}\right)\right|^2 \leq \lambda(N, Q) \sum_{n=M+1}^{N+M} |a_n|^2$$

Indeed applying Cauchy-Schwarz

$$\begin{aligned}\sum_{q\leq Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left|S\left(\frac{a}{q}\right)\right|^2 &= \sum_{q\leq Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left|\sum_{n=M+1}^{M+N} a_n e(na/q)\right|^2 \\ &\leq \sum_{q\leq Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \sum_{n=M+1}^{M+N} |a_n|^2 \\ &= \underbrace{\left(\sum_{q\leq Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} 1\right)}_{\lambda(N,Q)} \left(\sum_{n=M+1}^{M+N} |a_n|^2\right)\end{aligned}$$

What do we want from this inequality?

1. Find good functions λ which satisfies the inequality;
2. instantiate the inequality with parameters $N, M, Q, (a_n)$ of our choice to get bounds for particular expressions.

Best result

$$\lambda(N, Q) := N - 1 + Q^2$$

works, and this is the best possible bound that can be obtained.

Getting more general

Where are we summing over?

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2$$

$\frac{a}{q}$ are all rational number in $[0, 1]$ whose denominator in reduced form is $\leq Q$.
We denote this set with $\mathcal{F}_Q$

Observation

$\mathcal{F}_Q$ is equidistributed with level $1/Q^2$, i.e. for all $\alpha, \beta \in \mathcal{F}_Q$

$$||\alpha - \beta|| \geq \frac{1}{Q^2}.$$

We can rewrite the large sieve inequality in the following way:

$$\sum_{\alpha \in \mathcal{F}_Q} |S(\alpha)|^2 \leq \lambda(N, Q) \sum_{n=M+1}^{M+N} |a_n|^2$$

Observation

This new formulation suggests that we could try to establish the inequality with more general sets (maybe equidistributed).

We try to substitute $\mathcal{F}_Q$ with a general equidistributed $\mathcal{F}_\delta$.
We now look for a function $\lambda_0(N,\delta)$ s.t.

$$\sum_{\alpha\in\mathcal{F}_\delta} |S(\alpha)|^2 \le \lambda_0(N,\delta) \sum_{n=M+1}^{M+N} |a_n|^2$$

Observation

If we find a bound λ_0 for this inequality, then the large sieve inequality works with

$$\lambda(N,Q) = \lambda_0\left(N, \frac{1}{Q^2}\right)$$

Best result

$$\lambda_0(N, \delta) := N - 1 + \delta^{-1}$$

works, and this is the best possible bound that can be obtained.

The large sieve: applications

- (Bombieri) Basic mean value theorem;
- (Linnik) Distribution of quadratic nonresidues;
- (Rényi) Every large even number $2n$ can be expressed in the form

$$2n = p + P_k$$

where p is a prime and P_k is the product of at most k primes.

Recap
What did we see?

- Framework;
- tools:
  - Dirichlet characters;
  - large sieve inequality;
- main proof.

Thanks

Bibliography

Sahay, Anurag, and SRF Application No. “The Bombieri-Vinogradov Theorem.”

Park., Peter S. “The Bombieri–Vinogradov theorem.” Expository, preprint available http://web. math. princeton. edu/pspark/papers/bv. pdf (2016): 1-33.

Vaughan, R. C. “The Bombieri–Vinogradov Theorem.” (1965).