Brun's Sieve

Wenqi Li

February 22, 2024

Everything, except for some details, is contained in [FI10].

1 Basic Setup

Let $\mathcal{P}$ be a set of primes. We introduce the notation

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p.$$

The variable z is referred to as the sifting level. Note that $P(z)$ is a product of distinct primes, so we use the term "sifting range" to refer to both the number $P(z)$ and the primes that divides $P(z)$.

Let $\mathcal{A} = (a_n)$ be a sequence of non-negative real numbers. We define the "sifting function" as

$$S(\mathcal{A}, \mathcal{P}, z, x) = \sum_{\substack{n \leq x \\ (n, P(z)) = 1}} a_n$$

Often the restriction $n \leq x$ is imposed everywhere and understood from the context (or sometimes the sequence $\mathcal{A} = (a_n)$ is taken to be a finite sequence to begin with), so we may omit it and just write

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{(n, P(z)) = 1} a_n$$

When the set $\mathcal{P}$ is also understood, we omit the dependent on $\mathcal{P}$ too.

Recall that the Mobius function $\mu(n)$ is defined as

$$\mu(n) = \begin{cases} (-1)^r, & n = p_1 \cdots p_r \\ 0, & n \text{ is not squarefree} \end{cases}.$$

By convention $\mu(1) = 1$, since 1 is an empty product (i.e. $r = 0$). It is a basic fact that

$$\sum_{d \mid n} \mu(d) = 0$$

for any $n > 1$ and is equal to 1 if $n = 1$.

It follows that the condition $(n, P(z)) = 1$ can be detected by

$$\sum_{\substack{d|n \\ d|P(z)}} \mu(d) = \begin{cases} 1, & (n, P(z)) = 1 \\ 0, & \text{otherwise} \end{cases}.$$

This is because if $(n, P(z)) = 1$ then the sum has only one term $\mu(1) = 1$. Otherwise, the sum is just $\sum_{d|(n,P(z))} \mu(d) = 0$. Using this, we obtain

$$\begin{aligned} S(\mathcal{A}, z) &= \sum_{(n,P(z))=1} a_n \\ &= \sum_{n \le x} \left(a_n \sum_{\substack{d|n \\ d|P(z)}} \mu(d) \right) \\ &= \sum_{d|P(z)} \left(\mu(d) \sum_{d|n} a_n \right) \end{aligned}$$

Remember that we have the hidden condition $n \le x$, so all sums are finite and we can switch the order of summation. This motivates us to define the "congruence sums"

$$A_d(x) = \sum_{\substack{n \le x \\ d|n}} a_n.$$

So now

$$S(\mathcal{A}, z, x) = \sum_{d|P(z)} \mu(d) A_d(x)$$

Suppose X is some smooth approximation for $A_1(x) = \sum_{n \le x} a_n$, and assume we can write

$$A_d(x) = g(d)X + r_d(x).$$

Here, the idea is that $g(d)$ behaves like a probability density. We assume $g(1) = 1$, and g is multiplicative as an arithmetic function. We also assume that $g(d_1) \le g(d_2)$ if $d_2 | d_1$. With this expression for $A_d(x)$, we can write

$$S(\mathcal{A}, z, x) = \sum_{d|P(z)} \mu(d) g(d) X + \sum_{d|P(z)} \mu(d) r_d(x)$$

And to simply notation we define

$$V(z) = \sum_{d|P(z)} \mu(d) g(d).$$

By the multiplicativity assumption on g, we observe that

$$V(z) = \prod_{p|P(z)} (1 - g(p)).$$

2 Brun's Pure Sieve

Lemma 2.1 (Buchstab formula). *Keep the notation from the previous section. Let $\mathcal{A}_d$ denote the subset of $\mathcal{A}$ whose indices are divisible by d. We have*

$$S(\mathcal{A},z) = A_1(x) - \sum_{p|P(z)} S(\mathcal{A}_p,p) \tag{1}$$

Proof. The quantity $S(\mathcal{A},z)$ is obtained by first summing a_n over all $n \le x$, and then subtracting the ones whose indices are divisible by some prime factor of $P(z)$. The first is just $A_1(x)$. For each prime $p|P(z)$, the quantity $S(\mathcal{A}_p,p)$ is the sum of a_n whose indices are divisible by p but not divisible by any prime smaller than p. Going through the list of primes dividing $P(z)$ in increasing order gives the formula. ∎

Let $\omega(n)$ denote the number of prime divisors of n.

Lemma 2.2. *Let $p(d)$ denote the least prime divisor of d. Then each positive integer r, we have*

$$S(\mathcal{A},z) = \sum_{\substack{d|P(z)\\ \omega(d)<r}} \mu(d)A_d(x) + (-1)^r \sum_{\substack{d|P(z)\\ \omega(d)=r}} S(\mathcal{A}_d,p(d))$$

Proof. We use induction on r. When $r=1$, the equality is just (1) in Lemma 2.1. Now assume the desired equality is true for some r. Using Lemma 2.1, we have

$$S(\mathcal{A}_d,p(d)) = A_d(x) - \sum_{p|P(p(d))} S(\mathcal{A}_{pd},p)$$

The terms $(-1)^r A_d(x)$ is equal to $\mu(d)A_d(x)$ since in the second sum d has r distinct prime divisors. So we obtain

$$S(\mathcal{A},z) = \sum_{\substack{d|P(z)\\ \omega(d)<r+1}} \mu(d)A_d(x) + (-1)^{r+1} \sum_{\substack{d|P(z)\\ \omega(d)=r}} \sum_{p|P(p(d))} S(\mathcal{A}_{pd},p)$$

But if p divides $P(p(d))$, we must have $p < p(d)$, so p is the least prime divisor of pd, and pd has $r+1$ distinct prime divisors. The inner sum collects all the possible $(r+1)$-th prime divisors, so we obtain the desired equality for $r+1$. This completes the proof. ∎

We have a version of both Lemma 2.1 and Lemma 2.2 for the $V(z)$ function. From Lemma 2.1 we get that

$$XV(z) + \sum_{d|P(z)} \mu(d)r_d(x) = X + r_1(x) - \sum_{p|P(z)} \left(g(p)XV(p) + \sum_{d|P(p)} \mu(pd)r_{pd}(x) \right)$$

The remainder terms all cancel out, and dividing through by X we obtain

$$V(z) = 1 - \sum_{p|P(z)} g(p)V(p)$$

This is the Buchstab formula for $V(z)$. Similarly, applying it r times, we obtain

$$V(z) = \sum_{\substack{d|P(z) \\ \omega(d)<r}} \mu(d)g(d) + (-1)^r \sum_{\substack{d|P(z) \\ \omega(d)=r}} g(d)V(p(d)). \tag{2}$$

If we substitute $A_d(x) = g(d)X + r_d(x)$ into the formula in Lemma 2.2, we will get

$$S(\mathcal{A}, z) = \sum_{\substack{d|P(z) \\ \omega(d)<r}} \mu(d)g(d)X + \sum_{\substack{d|P(z) \\ \omega(d)<r}} \mu(d)r_d(x) + (-1)^r \sum_{\substack{d|P(z) \\ \omega(d)=r}} S(\mathcal{A}_d, p(d))$$

By (2), the first summation is equal to

$$XV(z) - X(-1)^r \sum_{\substack{d|P(z) \\ \omega(d)=r}} g(d)V(p(d)).$$

Therefore

$$S(\mathcal{A}, z) = XV(z) + \sum_{\substack{d|P(z) \\ \omega(d)<r}} \mu(d)r_d(x) + (-1)^r \sum_{\substack{d|P(z) \\ \omega(d)=r}} (S(\mathcal{A}_d, p(d)) - g(d)XV(p(d)))$$

We can use the crude bound $0 \le S(\mathcal{A}_d, p(d)) \le A_d(x)$ and $0 \le V \le 1$ to estimate the third term. It is between

$$(-1)^{r+1} X \sum_{\substack{d|P(z) \\ \omega(d)=r}} g(d)$$

and

$$(-1)^r X \sum_{\substack{d|P(z) \\ \omega(d)=r}} g(d) + (-1)^r \sum_{\substack{d|P(z) \\ \omega(d)=r}} r_d(x)$$

So in summary, if we let

$$G_r = \sum_{\substack{d|P(z) \\ \omega(d)=r}} g(d) \quad \text{and} \quad R_r = \sum_{\substack{d|P(z) \\ \omega(d)\le r}} |r_d(x)|$$

then

$$S(\mathcal{A}, z) = XV(z) + \theta X G_r + \theta R_r$$

for some $|\theta| \le 1$.

Notice that for G_1 we can estimate

$$G_1 = \sum_{p|P(z)} g(p) \le \sum_{p|P(z)} -\log(1 - g(p)) = -\log V(z).$$

Also we have the following observation:

Lemma 2.3. *For any $r \geq 1$,*

$$G_r \leq \frac{G_1^r}{r!}.$$

Proof. Expanding the product

$$G_1^r = \left(\sum_{p|P(z)} g(p)\right) \cdots \left(\sum_{p|P(z)} g(p)\right)$$

and use the multiplicativity of g, we see that for each $d|P(z)$, the term $g(d)$ appears $r!$ times where $r = \omega(d)$ is the number of distinct prime factors of d. Ignoring terms involving repeated factors and dividing by $r!$ gives the inequality. ■

An example

Now suppose $|r_d(\mathcal{A})| \leq g(d)d$ whenever $d|P(z)$. Then we have

$$R_r = \sum_{\substack{d|P(z)\\ \omega(d)\leq r}} |r_d(x)| \leq \sum_{\substack{d|P(z)\\ \omega(d)\leq r}} g(d)d$$

Again d is at most $z^{\omega(d)}$. Grouping together all possible $k = \omega(d)$, we have

$$\sum_{\substack{d|P(z)\\ \omega(d)\leq r}} g(d)d \leq \sum_{k=0}^{r} G_k z^k.$$

By Lemma 2.3, we get

$$R_r \leq \sum_{k=0}^{r} \frac{G_1^k}{k!} z^k \leq \sum_{k=0}^{r} A^r \left(\frac{zG_1}{A}\right)^k \frac{1}{k!} = A^r e^{zG/A}$$

for any $A \geq 1$. In particular, we take $A = \max(1, zG/r)$. If $zG/r \geq 1$, then substituting A we get $A^r e^{zG/A} = (zG/r)^r e^r$, and if $zG/r < 1$ then $zG < r$, so $A^r e^{zG/A} = e^{zG} < e^r$. In any case

$$R_r \leq (zeG/r)^r + e^r$$

Recall that we showed

$$G_r \leq \frac{1}{e}\left(\frac{eG}{r}\right)^r$$

Therefore using our new estimates for R_r, we get

$$|S(\mathcal{A}, z) - XV(z)| \leq \frac{X}{e}\left(\frac{eG}{r}\right)^r + \left(\frac{zeG}{r}\right)^r + e^r \leq \left(\frac{eG}{r}\right)^r (X + z^r) + e^r$$

Now we choose $r = [\log X / \log z]$, so in the above bound z^r becomes X. Recall that $G \leq |\log V|$. When

$$4 \leq z \leq X^{1/c\log(V^{-1}\log X)} \tag{3}$$

we have that

$$\log z \leq \log X / c \log(V^{-1} \log X)$$

so

$$r \geq c \log(V^{-1} \log X), \text{i.e. } e^{r/c} \geq V^{-1} \log X.$$

We want to the inequality

$$\left(\frac{e \log V^{-1}}{r}\right)^r \leq e^{-r/c} \tag{4}$$

Taking log, this is

$$r(1 + \log\log V^{-1} - \log r) \leq \frac{-r}{c}$$

When $r = c\log(V^{-1}\log X)$, the right side is $-\log(V^{-1}\log X)$. The left side is

$$c\log(V^{-1}\log X)(1+\log\log V^{-1}-\log c-\log\log(V^{-1}\log X)) = \log(V^{-1}\log X)(-1-\log\log\log X)$$

which is smaller than the right side. The derivative of the left side is negative and decreasing, so for r greater than the said value, we always have the inequality (4). The inequality (4) implies

$$\left(\frac{eG}{r}\right)^r \leq V(z)(\log X)^{-1}$$

The derivation in teal is not reliable and unimportant. The conclusion is that when (3) is satisfied, we have that

$$|S(\mathcal{A}, z) - XV(z)| \leq 2V(z)X(\log X)^{-1} + X^{\frac{3}{4}} \tag{5}$$

Let us now see why these nasty formulas are useful. Let F be a polynomial that is a product of k distinct irreducible polynomials over $\mathbf{Z}$ with positive leading coefficient. Let the sequence $\mathcal{A}$ be the indicator sequence for $F(m)$ for $1 \leq m \leq x$. This is a sieve of dimension k, and using generalities in Chapter 5 of [FI10], we have that $V(z)^{-1} \leq (K\log x)^k$, which implies $V(z) \asymp (\log z)^{-k}$. Let

$$\pi_F(x, z) = \#\{1 \leq m \leq x \mid (F(m), P(z)) = 1\}$$

This is just $S(\mathcal{A}, z)$. Then using (5), we get

$$\pi_F(x, z) \asymp x(\log z)^{-k}$$

provided that

$$4 \leq z \leq x^{\frac{1}{c}(k+1)\log(K\log x)}$$

i..e $\log z \ll \log x \log\log x$. This implies that

$$\pi_F(x) \ll x\left(\frac{\log\log x}{\log x}\right)^k$$

For $F(m) = m(m-2)$, we established an upper bound for the number of twin primes $\pi_2(x)$ up to x. This implies that the sum of reciprocals of twin primes converges.

3 Sifting Weights

So far we have only used the "pure" sieve: we rewrote the summation over the condition $(n,P(z))=1$ in terms of the Mobius function. More sophisticated sieves replace the Mobius function $\mu(d)$ by some other (truncated) sequence $\Lambda=(\lambda_d)$. In particular, if the sequence λ_d is all 0 after $d \geq D$ for some D, we say that (λ_d) is a choice of sifting weights (or sieve weights) of level D. We refer to the ratio

$$s=\frac{\log D}{\log z}$$

as the sifting variable.

We had $S(\mathcal{A},z)=\sum_{d|P(z)}\mu(d)A_d(x)$, but with different sifting weights we won't have this equality. Instead, we defined the sifted sum

$$S^{\Lambda}(\mathcal{A},z)=\sum_{d|P(z)}\lambda_d A_d(x).$$

We see that with $\theta=1\star\lambda$, i.e. $\theta_n=\sum_{d|n}\lambda_d$, we have

$$S^{\Lambda}(\mathcal{A},z)=\sum_n a_n\theta_n$$

If Λ makes $S^{\Lambda}(\mathcal{A},z)$ a upper (resp. lower) bound for $S(\mathcal{A},z)$, then we say that Λ is an upper (resp. lower) bound sieve.

Definition 3.1. A choice of sifting weights (λ_d) gives a combinatorial sieve if λ_d takes only the values $\mu(d)$ and 0.

In the previous section, we used a combinatorial sieve controlled by the parameter r. The parity of r determines whether it is an upper bound sieve or a lower bound sieve. Now we will construct upper bound and lower bound sieves using a different method of Brun.

This method is again motivated by the Buchstab formula:

$$S(\mathcal{A},z)=A_1(x)-\sum_{p_1|P(z)}S(\mathcal{A}_{p_1},p_1)$$

We wrote p_1 since we are going to do apply this procedure many times. If p_1 is large, the subsequence $\mathcal{A}_{p_1}$ will contain few terms, so maybe dropping these terms won't hurt much. In any case, we can choose some y_1 as the criterion of being "large", and obtain an upper bound

$$S(\mathcal{A},z)\leq A_1(x)-\sum_{\substack{p_1|P(z)\\ p_1<y_1}}S(\mathcal{A}_{p_1},p_1).$$

As long as $y_1\leq P(z)$, we can drop the $p_1|P(z)$ condition. Now we can apply the Buchstab formula again to get

$$A_1(x)-\sum_{p_1<y_1}A_{p_1}(x)+\sum_{p_2<p_1<y_1}S(\mathcal{A}_{p_1p_2},p_2)$$

Nothing can be done here: we can't ignore p_2's that are larger than a certain value, because they are positive terms and we are in the process of finding an upper bound. However, applying the Buchstab formula again, we can ignore p_3's that are larger than some y_3:

$$S(\mathcal{A},z) \leq A_1(x) - \sum_{p_1<y_1} A_{p_1}(x) + \sum_{p_2<p_1<y_1} A_{p_1p_2}(x) - \sum_{p_3<y_3<p_2<p_1<y_1} S(\mathcal{A}_{p_1p_2p_3},p_3)$$

So we see that for m odd, we can set some y_m, and only consider $p_m < y_m$ in that step of the Buchstab iteration. This motivates us to fix a sequence of these y_m, and define

$$\mathcal{D}^+ = \{d = p_1 \cdots p_l \mid p_m < y_m \text{ for } m \text{ odd}\}.$$

The prime factors $p_1, \cdots, p_l$ are always ordered in decreasing order. Notice that this is a finite set since p_1 is bounded. (This comment is actually meaningless since we always implicitly intersect with the divisors of $P(z)$, but it is easy to get confused here.)

We get

$$S(\mathcal{A},z) \leq \sum_{\substack{d|P(z)\\ d\in\mathcal{D}^+}} \mu(d)A_d(x) = S^+(\mathcal{A},z) \tag{6}$$

Note that in the last step of such iteration, i.e. we have used all primes smaller than p_1, then the smallest one p_l must be 2, and $S(\mathcal{A},2)$ is just the sum of $\mathcal{A}$, so the bound above has no leftover terms on the right side, unlike when the process has not terminated.

What did we lose? At each odd n, we ignored

$$S_n(\mathcal{A},z) = \sum_{\substack{y_n\leq p_n<\cdots<p_1\\ p_m<y_m, m<n, m \text{ odd}}} S(\mathcal{A}_{p_1\cdots p_n},p_n)$$

So actually

$$S(\mathcal{A},z) = S^+(\mathcal{A},z) - \sum_{n \text{ odd}} S_n(\mathcal{A},z).$$

Similarly, we can define

$$\mathcal{D}^+ = \{d = p_1 \cdots p_l \mid p_m < y_m \text{ for } m \text{ even}\}.$$

and obtain a lower bound

$$S(\mathcal{A},z) \geq \sum_{\substack{d|P(z)\\ d\in\mathcal{D}^-}} \mu(d)A_d(x) = S^-(\mathcal{A},z) \tag{7}$$

A completely analogous procedure can be carried out for the V function. Recall that

$$V(z) = \sum_{d|P(z)} \mu(d)g(d) = \prod_{p|P(z)} (1-g(p))$$

and using the procedure described above we obtain

$$V(z) = V^+(D,z) - \sum_{n \text{ odd}} V_n(z)$$

where

$$V^+(D,z) = \sum_{\substack{d|P(z) \\ d\in\mathcal{D}^+}} \mu(d)g(d)$$

and

$$V_n(z) = \sum_{\substack{y_n \le p_n < \cdots < p_1 < z \\ p_m < y_m, m<n, m \text{ odd}}} g(p_1 \cdots p_n)V(p_n).$$

The question now is how to choose the truncating parameters y_m appropriately. A possible choice is

$$y_m = \left(\frac{D}{p_1 \cdots p_m}\right)^{\frac{1}{\beta}}.$$

A sieve given by these parameters is called a beta-sieve of level D. Note that for a different number of final stage, these parameters will be different. We will not cover the reason behind this choice.

4 The Fundamental Lemma

Suppose we selected the parameters y_m according to some fixed β and D.

We only need upper bounds for $V_n(z)$. The summation condition of V_n is complicated, but the terms are non-negative, so we will try to simplify the summation condition at the cost of summing more terms.

Lemma 4.1. *Suppose $p_1 > \cdots > p_n$ satisfies the summation condition for $V_n(z)$. Then for any $1 \le \ell \le n-1$ and $\ell \equiv n-1 \bmod 2$, we have*

$$p_1 \cdots p_l < Dz^{\epsilon_\ell}$$

where $\epsilon_\ell = -(s-1)\left(\frac{\beta-1}{\beta+1}\right)^{[\ell/2]}$.

Proof. We use induction on ℓ. We know that $\ell - 1 \equiv n \bmod 2$, so $p_{\ell-1} < y_{\ell-1}$, and thus

$$p_1 \cdots p_{\ell-2} p_{\ell-1}^{\beta+1} < D.$$

Now use $p_\ell < p_{\ell-1}$ to get

$$p_1 \cdots p_\ell < p_1 \cdots p_{\ell-2} p_{\ell-1}^2 < p_1 \cdots p_{\ell-2}\left(\frac{D}{p_1 \cdots p_{\ell-2}}\right)^{2/(\beta+1)}$$

and use the induction hypothesis. ■

Corollary 4.2. *Suppose $p_1 > \cdots > p_n$ satisfies the summation condition for $V_n(z)$. Then*

$$p_n \ge z^{\delta_n}$$

where

$$\delta_n = \frac{s-1}{\beta-1}\left(\frac{\beta-1}{\beta+1}\right)^{[(n+1)/2]}$$

Proof. Apply the previous lemma with $\ell = n-1$ we get

$$p_1 \cdots p_{n-1} < Dz^{-(s-1)\left(\frac{\beta-1}{\beta+1}\right)^{[(n-1)/2]}}$$

So

$$p_n \geq y_n = \left(\frac{D}{p_1 \cdots p_n}\right)^{\frac{1}{\beta}} \geq z^{\frac{s-1}{\beta}\left(\frac{\beta-1}{\beta+1}\right)^{[(n-1)/2]}} p_n^{-1/\beta}$$

Rearranging gives the desired inequality. ■

Assuming $s \geq \beta+1$, we let $z_n = z^{\left(\frac{\beta-1}{\beta+1}\right)^{n/2}}$, and the Corollary implies $p_n \geq z_n$ provided that the p_i's satisfy the summation condition. Therefore, we can drop all those condition and only require $p_n \geq z_n$ to get an upper bound

$$V_n(z) \leq \sum_{z_n \leq p_n < \cdots < p_1 < z} g(p_1 \cdots p_n) V(p_n).$$

Theorem 4.3 (The Fundamental Lemma). *Suppose we have a beta sieve with dimension κ and $\beta = 9\kappa+1$. Assume the function g satisfies*

$$\prod_{w \leq p < z} (1-g(p))^{-1} \leq K\left(\frac{\log z}{\log w}\right)^{\kappa}$$

and $s \geq 9\kappa+1$. Then

$$V^+(D,z) \leq (1+e^{9\kappa-s}K^{10})V(z).$$

Proof. We obtained that

$$V_n(z) \leq \sum_{z_n \leq p_n < \cdots < p_1 < z} g(p_1 \cdots p_n) V(p_n)$$

Notice that $V(p_n) \leq V(z_n)$ since V is a product of terms less than 1. Then, using the same proof as in Lemma 2.3, we get that

$$\sum_{z_n \leq p_n < \cdots < p_1 < z} g(p_1 \cdots p_n) V(p_n) \leq V(z_n) \frac{1}{n!}\left(\sum_{z_n \leq p \leq z} g(p)\right)^n$$

For each $g(p)$ we use the inequality $g(p) \leq -\log(1-g(p))$, and we get the above is bounded above by

$$\frac{V(z_n)}{n!}\left(\log \frac{V(z_n)}{V(z)}\right)^n$$

Our assumption implies that

$$\frac{V(z_n)}{V(z)} \leq K(\frac{\log z}{\log z_n})^{\kappa}$$

Remembering the definition of z_n, we have $\frac{\log z}{\log z_n} = \left(\frac{\beta+1}{\beta-1}\right)^{n/2}$. To simplify notation, let $\alpha = \frac{\kappa}{2}\log\frac{\beta+1}{\beta-1}$. Then

$$\frac{V_n(z)}{V(z)} \leq \frac{K}{n!}(e^{\alpha}\log(Ke^{\alpha n}))^n = \frac{K}{n!}(e^{\alpha}\log K + e^{\alpha}\alpha n)^n$$

We estimate

$$e^{\alpha}(\log K + \alpha n) = e^{\alpha}\alpha n(1 + \frac{\log K}{\alpha n}) \leq e^{\alpha}\alpha n \exp(\frac{\log K}{\alpha n}) = e^{\alpha}\alpha n K^{\frac{1}{\alpha n}}.$$

So in summary

$$\frac{V_n(z)}{V(z)} \leq \frac{1}{n!}(e^{\alpha}\alpha n)^n K^{1+\frac{1}{\alpha}}.$$

Now sum this over n, choose β appropriately ($\beta = 9\kappa+1$), and get the desired bound. ■

Let's apply this to the $\pi_F(x,z)$ example considered in section 2. Recall that F is a polynomial that is a product of k distinct irreducible polynomials over $\mathbf{Z}$, and $\mathcal{A}$ is the indicator sequence for $F(m)$ for $1 \leq m \leq x$. To apply our beta sieve, we let $D = x = X$ and $\kappa = k$. So the fundamental lemma implies that $\pi_F(x,z) \asymp XV(z) = x(\log z)^{-k}$, provided that $z^{9\kappa+1} \leq D$. This means that we are trying to consider all primes up to $D = x$ and sift out their multiples, but our estimate is only true (to our knowledge) when we only sift out not so many prime. However, we still have $\log z \ll \log D = \log x$, so we obtain

$$\pi_F(x,z) \ll x(\log x)^{-k}.$$

Notice that this is a big improvement comparing to the result in section 2: we get rid of the $(\log\log x)^k$ factor.

In fact, by being slightly more careful, we obtain

Theorem 4.4. *We have*

$$\pi_F(x,z) \asymp x(\log z)^{-k}$$

for $x \geq z^{9k+1}$. *In particular, there are infinitely many pairs of integers* m *and* $m-2$ *such that together they have at most* 19 *prime divisors.*

Proof. The general estimate is what we got before we substituted $\log z \ll \log x$. Now let $F(m) = m(m-2)$, so $k = 2$ and $9k+1 = 19$. Then the estimate says that for x large enough, in the range $[0,x]$, the number of integers of the form $m(m-2)$ where no prime smaller than z divides $m(m-2)$ is at least a constant multiple of $x(\log z)^{-k}$. We may choose z to be close to $x^{1/19}$, so so any such $m(m-2) < x$ cannot have more than 19 prime divisors, since these divisors are all at least $x^{1/19}$. Now taking x to infinity gives the infinitude result.

■

In fact, with some more estimates, one can show this result for 9 primes, rather than 19. This is done in the book. Other refinements of Brun's sieve can reduce this number to 4. This illustrates the power of these sieves in attacking the twin prime conjecture.

References

[FI10] J.B. Friedlander and H. Iwaniec. *Opera de Cribro*. American mathematical society colloquium publications. American Mathematical Society, 2010. ISBN: 9780821849705.