

Решето А. Сельберга

Атле Сельбергу (1917 - 2007) принадлежит простой и красивый способ верхней оценки просеиваемой функции

$$S(A, P, z) = \sum_{\substack{n \leq x \\ (n, P(z))=1}} a_n = \sum_{n \leq x} a_n \left(\sum_{d|n, P(z)} \mu(d) \right),$$

который впоследствии получил название "решето Сельберга". В отличие от решета Бруна, где носительности коэффициентов $\sum_{d|m} \lambda_d^+$, метри-

рующих $\sum_{d|m} \mu(d)$ при любом n , достигается за счет достаточно простых рассуждений, в решете Сельберга это делается почти автоматически.

Зададимся величиной z и обозначим $D = z^2$ (число D будет в дальнейшем играть ту же роль, что и одноименная величина в решете Бруна; там z и D были связаны равенством вида $D = z^{2\theta+4}$).

Величина D будет отвечать за "носителя" λ_d^+ ; именно, скажем, что $\lambda_d^+ \equiv 0$ для всех $d > D$. Иногда параметр D называют "уровнем распределения" ("level distribution"; преимуществ. в англоязычной литературе).

Пусть теперь ρ_d — произвольная последовательность вещественных чисел с носителем на отрезке $[1, z]$ (т.е. $\rho_d \equiv 0$ для всех $d > z$), удовлетворяющая (пока) единственному условию $\rho_1 = 1$. Определим величины λ_d так, чтобы при любом $n \geq 1$ число

$$\sum_{d|n} \lambda_d = \left(\sum_{d|n} \rho_d \right)^2 \quad (1)$$

Очевидно тогда, что

$$\left(\sum_{d|n} \rho_d \right)^2 \geq \sum_{d|n} \mu(d)$$

для всякого $n \geq 1$, так что можно положить $\lambda_d^+ = \lambda_d$.

Выразим λ_d через ρ_d . Имеем:

$$\left(\sum_{d|n} \rho_d \right)^2 = \sum_{d_1, d_2 | n} \rho_{d_1} \rho_{d_2} = \sum_{d|n} \sum_{\substack{d_1, d_2 | n \\ [d_1, d_2] = d}} \rho_{d_1} \rho_{d_2}, \text{ т.е.}$$

определение (1) равносильно соотношению

$$\lambda_d = \sum_{\substack{d_1, d_2 | n \\ [d_1, d_2] = d}} \rho_{d_1} \rho_{d_2}$$

Возвращаясь к исходной функции, получим:

$$\begin{aligned} S(A, \rho, z) &\leq \sum_{n \leq \infty} a_n \left(\sum_{d|(n, P(z))} \rho_d \right)^2 = \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} \sum_{\substack{n \leq \infty \\ n \equiv 0 \pmod{d_1} \\ n \equiv 0 \pmod{d_2}}} a_n = \\ &= \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} \sum_{\substack{n \leq \infty \\ n \equiv 0 \pmod{[d_1, d_2]}}} a_n = \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} |A_{[d_1, d_2]}| \end{aligned}$$

Обозначим сумму в правой части переключенка через $S^+(A, z)$. Заметим, что в сумме по d_1, d_2 условие $d_1, d_2 < z$ опускается (для сохранения записи): в силу сделанного выше соглашения о носителе ρ_d слагаемые, отвечающие $d_1 > z$ или $d_2 > z$, автоматически отбрасываются.

Согласно "условию g" (которое предполагается выполненным для рассматриваемой последовательности $\{a_n\}$),

$$|A_{[d_1, d_2]}| = X g([d_1, d_2]) + z [d_1, d_2],$$

так что

$$S^+(A, z) = \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} (X g([d_1, d_2]) + z [d_1, d_2]) =$$

$$= XH + R^+, \text{ где}$$

$$H = \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} g([d_1, d_2]), \quad R^+ = \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} z [d_1, d_2]$$

Отметим, что для величины R^+ иногда используют обозначение $R^+(A, \Lambda^2)$, где обозначение Λ^2 возникает по традиции: в силу (1), решето Селберга называют иногда Λ^2 -решетом.

Естественно выбирать коэффициенты ρ_d так, чтобы мы минимизировать выражение $S^+(A, z)$. Однако эта задача в общем случае представляется очень сложной, и поэтому её заменяют более простой: выбирают ρ_d так, чтобы минимизировать одну лишь сумму H .

Сумма H является квадратичной формой от переменных ρ_d , где $1 \leq d \leq z$, $d | P(z)$. Заменой переменных её можно привести к диагональному виду.

Для этого заметим следующее. Поскольку оба числа d_1 и d_2 — бесквадратные, то в равенстве

$$[d_1, d_2] = \frac{d_1 d_2}{(d_1, d_2)} = \frac{d_1}{(d_1, d_2)} \cdot d_2 \quad \text{числа}$$

$\frac{d_1}{(d_1, d_2)}$ и d_2 — взаимно-простые, так что

$$g([d_1, d_2]) = g\left(\frac{d_1}{(d_1, d_2)}\right) g(d_2).$$

Вновь используя тем, что d_1 и d_2 — бесквадратные, находим:

$$g\left(\frac{d_1}{(d_1, d_2)}\right) = \frac{g(d_1)}{g((d_1, d_2))}.$$

Поэтому окончательно имеем:

$$g([d_1, d_2]) = \frac{g(d_1) g(d_2)}{g((d_1, d_2))},$$

$$H = \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} g(d_1) g(d_2) \frac{1}{g((d_1, d_2))}$$

Определим теперь мультипликативную функцию $h(n)$ на бесквадратных n, d ($d | P(z)$) соотношением

$$\frac{1}{g(d)} = \sum_{n|d} \frac{1}{h(n)}.$$

По формуле обращения Мёбиуса,

$$\begin{aligned} \frac{1}{h(n)} &= \sum_{d|n} \mu(d) \frac{1}{g(\frac{n}{d})} = \frac{1}{g(n)} \sum_{d|n} \mu(d) g(d) = \\ &= \frac{1}{g(n)} \prod_{p|n} (1 - g(p)) = \prod_{p|n} \frac{1 - g(p)}{g(p)}. \end{aligned}$$

В частности, для простых $p | P(z)$ имеем

$$h(p) = \frac{g(p)}{1 - g(p)} \Rightarrow g(p) = \frac{h(p)}{1 + h(p)} \quad (2)$$

Так находим:

$$\begin{aligned} H &= \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} g(d_1) g(d_2) \sum_{\delta | (d_1, d_2)} \frac{1}{h(\delta)} = \\ &= \sum_{\delta | P(z)} \frac{1}{h(\delta)} \sum_{\substack{d_1, d_2 | P(z) \\ d_1, d_2 \equiv 0 \pmod{\delta}}} \rho_{d_1} g(d_1) \cdot \rho_{d_2} g(d_2) = \\ &= \sum_{\delta | P(z)} \frac{1}{h(\delta)} \left(\sum_{\substack{d | P(z) \\ d \equiv 0 \pmod{\delta}}} \rho_d g(d) \right)^2 = \sum_{\delta | P(z)} \frac{x_\delta^2}{h(\delta)}, \end{aligned}$$

где новые переменные x_δ для $\delta | P(z)$ определяем:

$$x_\delta = \sum_{\substack{d | P(z) \\ d \equiv 0 \pmod{\delta}}} \rho_d g(d).$$

Заметим, что при $\delta > z$ условие на носитель ρ_d автоматически даёт: $x_\delta \equiv 0$.

Выведем теперь формулы, выражающие ρ_d через x_δ . Для этого воспользуемся следующим приёмом, пригодным формулам обращения Мёбиуса. Именно, пусть последовательности

$A(n)$ и $B(n)$ связаны соотношением

$$A(n) = \sum_{\substack{m \leq x \\ m \equiv 0 \pmod{n}}} B(m).$$

Тогда $B(n) = \sum_{d \leq \frac{x}{n}} \mu(d) A(dn)$. Действительно, если n дано, то

$$\begin{aligned} \sum_{d \leq \frac{x}{n}} \mu(d) A(dn) &= \sum_{dn \leq x} \mu(d) \sum_{kdn \leq x} B(kdn) = \\ &= \sum_{kdn \leq x} \mu(d) B(kdn) = \sum_{\substack{r \leq \frac{x}{n} \\ d|r}} B(rn) \sum_{d|r} \mu(d) = B(n). \end{aligned}$$

Применяя эти формулы в случае $A(n) = x_n$, $B(n) = g_n g(n)$, получим:

$$B(n) = g_n g(n) = \sum_{\substack{d \leq \frac{x}{n} \\ d | P(z)}} \mu(d) x_{nd},$$

$$g_n = \frac{1}{g(n)} \sum_{d | P(z)} \mu(d) x_{nd}$$

(условие $d \leq \frac{x}{n}$ в последней сумме можно опустить, т.к. при $dn > x$ числа x_{nd} в силу сделанных выше замечаний, равны нулю).

В частности, условие $g_1 = 1$ принимает теперь вид

$$\sum_{d | P(z)} \mu(d) x_d = 1 \quad (3)$$

Итак, имеем следующую задачу: отыскать минимум квадратичной формы H ,

$$H = \sum_{\delta | P(z)} \frac{x_\delta^2}{h(\delta)},$$

при условии (3). Этот минимум может быть найден различными способами:

Способ первый: метод неопределенных множителей Лагранжа. Чтобы найти экстремум формы H при помощи "уравнения связи"

$$f = \sum_{d|P(z)} \mu(d) x_d - 1 = 0,$$

необходимо составить функцию $F(\bar{x}) = H + \lambda f$ (здесь $\bar{x}$ — набор переменных x_d , $d|P(z)$, $d \leq z$) и решить систему уравнений $\frac{\partial F(\bar{x})}{\partial x_d} = 0$. Имеем:

$$\frac{\partial F}{\partial x_d} = \frac{\partial H}{\partial x_d} - \lambda \frac{\partial f}{\partial x_d} = \frac{2x_d}{h(d)} - \lambda \mu(d) = 0,$$

откуда $x_d = \frac{\lambda}{2} \mu(d) h(d).$

Значение неопределенного множителя λ найдем из уравнения связи (3):

$$\sum_{d|P(z)} \mu(d) \cdot \frac{\lambda}{2} \mu(d) h(d) = \frac{\lambda}{2} \sum_{d|P(z)} \mu^2(d) h(d) = 1,$$

$$\frac{\lambda}{2} = \left(\sum_{d|P(z)} \mu^2(d) h(d) \right)^{-1}. \quad \text{Следовательно, координаты точки, доставляющей условный экстремум}$$

формы H , задаются формулами

$$x_d = \frac{\mu(d) h(d)}{\sum_{d|P(z)} \mu^2(d) h(d)} \quad (4)$$

Соответственно, значение формы H в точке экстремума равно

$$H = \sum_{d|P(z)} \frac{1}{h(d)} \cdot \frac{\mu^2(d) h^2(d)}{\left(\sum_{d|P(z)} \mu^2(d) h(d) \right)^2} = \frac{\sum_{d|P(z)} \mu^2(d) h(d)}{\left(\sum_{d|P(z)} \mu^2(d) h(d) \right)^2}$$

$$= \frac{1}{G(z)}, \quad \text{где } G(z) = \sum_{\substack{d|P(z) \\ d \leq z}} \mu^2(d) h(d).$$

(условие $d \leq z$ в определении суммы $G(z)$ можно так же опустить: из (4) следует, что $h(d) \equiv 0$ для всех $d > z$).

Чтобы доказать, что найденные значения x_d

доставляют именно минимум, необходимо дополнить рассуждения. В данном случае несложно проверить, что для сколь угодно большого числа N можно отыскать набор переменных $\bar{x}$, удовлетворяющих уравнению связи (3), на котором форма H принимает значение, превосходящее N : $H(\bar{x}) > N$ (проделайте это!)

Способ второй: неравенство Коши.

Имеем:

$$1 = \sum_{d|P(z)} \mu(d) x_d = \sum_{d|P(z)} \mu(d) \sqrt{h(d)} \cdot \frac{x_d}{\sqrt{h(d)}},$$

откуда в силу неравенства Коши получим:

$$1 \leq \left(\sum_{d|P(z)} \mu^2(d) h(d) \right) \cdot \left(\sum_{d|P(z)} \mu^2(d) \frac{x_d^2}{h(d)} \right) = GH.$$

Следовательно, $H \geq \frac{1}{G(z)}$. Неравенство обратится в равенство, если последовательности $\mu(d) \sqrt{h(d)}$ и $\frac{x_d}{\sqrt{h(d)}}$ прямо пропорциональны:

$$\frac{x_d}{\sqrt{h(d)}} = c \mu(d) \sqrt{h(d)}, \quad x_d = c \mu(d) h(d).$$

Коэффициент пропорциональности c определяется из уравнения связи (3):

$$\sum_{d|P(z)} \mu(d) \cdot c \mu(d) h(d) = 1, \quad c = \left(\sum_{d|P(z)} \mu^2(d) h(d) \right)^{-1} = \frac{1}{G(z)}.$$

Отсюда получаем введенные ранее формулы для x_d и H . Достоинство этого способа состоит в том, что из вышеприведенных рассуждений автоматически следует, что $\frac{1}{G(z)}$ будет минимальной формой H .

Выведем теперь формулы для коэффициентов ρ_d (они, кстати, часто называются коэффициентами Селберга). Для $n \leq z$, $n | P(z)$ имеем:

$$\rho_n = \frac{1}{g(n)} \sum_{\substack{d | P(z) \\ d \leq \frac{z}{n}}} \mu(d) x_{nd}.$$

Следовательно,

$$\rho_n = \frac{1}{g(n)} \sum_{\substack{d | P(z) \\ d \leq \frac{z}{n}}} \mu(d) \frac{\mu(dn) h(dn)}{G(z)} = \frac{\mu(n) h(n)}{g(n) G(z)} \sum_{\substack{d | P(z) \\ d \leq \frac{z}{n} \\ (d, n) = 1}} \mu^2(d) h(d)$$

Далее, для указанного n имеем:

$$\frac{h(n)}{g(n)} = \prod_{p | n} \frac{h(p)}{g(p)} = \prod_{p | n} \frac{g(p)}{1 - g(p)} \cdot \frac{1}{g(p)} = \prod_{p | n} \frac{1}{1 - g(p)}$$

Согласно формуле (2),

$$\frac{1}{1 - g(p)} = \frac{1}{1 - \frac{h(p)}{1 + h(p)}} = 1 + h(p), \text{ так что}$$

$$\frac{h(n)}{g(n)} = \prod_{p | n} (1 + h(p)) = \sum_{\delta | n} \mu^2(\delta) h(\delta),$$

Поэтому, возвращаясь к выражению для ρ_n найдем:

$$\begin{aligned} \rho_n &= \frac{\mu(n)}{G(z)} \sum_{\delta | n} \mu^2(\delta) h(\delta) \sum_{\substack{d | P(z) \\ dn \leq z, (d, n) = 1}} \mu^2(d) h(d) = \\ &= \frac{\mu(n)}{G(z)} \sum_{\substack{\delta | n \\ dn \leq z, (d, n) = 1}} \sum_{d | P(z)} \mu^2(d\delta) h(d\delta). \end{aligned}$$

Заметим, что всякое число n , $1 \leq n \leq z$, $n | P(z)$, единственным образом представимо в виде произведения $n = d\delta$, где $\delta | n$, и $(d, n) = 1$.
Значит, среди чисел $n = d\delta$, встречающихся в последнем выражении для ρ_n , нет пов-

порений, и каждое из них не превосходит z .
Очевидно, все такие n встречаются и в сумме $G(z)$, стоящей в знаменателе.

Контрольный вопрос: а какие слагаемые присутствуют в $G(z)$, но отсутствуют в сумме по $d \leq z$?

Итак,
$$|g_m| \leq \frac{1}{G(z)} \cdot G(z) = 1.$$

Переходя к оценке остаточного члена, будем иметь:

$$|R^+| \leq \left| \sum_{d_1, d_2 | P(z)} g_{d_1} g_{d_2} \tau[d_1, d_2] \right| \leq \sum_{d_1, d_2 | P(z), d_1, d_2 \leq z} |\tau[d_1, d_2]| =$$

$$= \sum_{\substack{d | P(z) \\ d \leq z^2}} |\tau_d| \sum_{\substack{d_1, d_2 | P(z) \\ [d_1, d_2] = d}} 1 = \sum_{\substack{d | P(z) \\ d \leq \mathfrak{D}}} |\tau_d| \cdot u(d),$$

где обозначено: $u(d) = \sum_{\substack{d_1, d_2 | d \\ [d_1, d_2] = d}} 1$. Для бес-
численного $u(d)$

зафиксируем делитель d_1 числа d , так что $d = d_1 \delta$. Тогда все делители d_2 с условием $[d_1, d_2] = d$ должны иметь вид $m \delta$, где $m | d_1$, но их количество совпадает с числом способов образования m , которое, очевидно, равно d_1 . Итак,

$$u(d) = \sum_{d_1 | d} \tau(d_1) = \tau_3(d).$$

В частности, для бесквадратного d имеем:

$$u(d) = 3^{\omega(d)}, \quad \text{Итак,}$$

$$|R^+| \leq \sum_{\substack{d \leq \mathfrak{D} \\ d | P(z)}} 3^{\omega(d)} |\tau_d|$$

Итак, нами доказана основная теорема решета
Сельберга:

Теорема 1 Пусть для последовательности $A = \{a_n\}$, множества простых чисел P выполнено "условие", причем $0 \leq g(p) < 1$ для всякого $p \in P$. Тогда при любом z , $2 \leq z \leq x$, для просеиваемой функции вып. кер-во:

$$S(A, P, z) \leq \frac{X}{G(z)} + \sum_{\substack{d|P(z) \\ d \leq D}} \omega(d) |z_d|,$$

в котором $D = z^2$, $G(z) = \sum_{\substack{d|P(z) \\ d \leq z}} \mu^2(d) h(d)$,

причем $h(d)$ — мультипликативная функция, определенная на всех простых числах $p \in P$ равенством

$$h(p) = \frac{g(p)}{1 - g(p)}$$

В некоторых случаях можно указать явный вид оценки остаточного члена в неравенстве для $S(A, P, z)$, более удобный для приложения.

Теорема 2. Пусть выполнены условия Теоремы 1 и при этом $|z_d| \leq C$ для всех d , $d|P(z)$, где C — постоянная. Тогда

$$S(A, P, z) \leq \frac{X}{G(z)} + Cz^2$$

Док-во. Необходимо лишь заметить, что

$$|R^+| \leq \sum_{\substack{d_1, d_2 | P(z), \\ d_1, d_2 \leq z}} |z_{[d_1, d_2]}| \leq C \sum_{d_1, d_2 \leq z} 1 = Cz^2.$$

Теорема 3. Пусть выполнены условия Теоремы 1 и при этом $|z_d| \leq C d g(d)$ для всех d , $d|P(z)$, где C — постоянная. Тогда

$$S(A, P, z) \leq \frac{X}{G(z)} + \frac{Cz^2}{V^3(z)}, \quad V(z) = \prod_{\substack{p \leq z \\ p \in P}} (1 - g(p)).$$

Док-во. Согласно Теореме 1, имеем:

$$\begin{aligned}
 |R^+| &\leq \sum_{\substack{d|P(z) \\ d \leq z^2}} 3^{\omega(d)} |z_d| \leq C \sum_{\substack{d|P(z) \\ d \leq z^2}} 3^{\omega(d)} d g(d) \leq C z^2 \sum_{\substack{d|P(z) \\ d \leq z^2}} 3^{\omega(d)} g(d) = \\
 &= C z^2 \prod_{\substack{p \leq z \\ p \in P}} (1 + 3g(p)) \leq C z^2 \prod_{\substack{p \leq z \\ p \in P}} (1 + g(p))^3 \leq \\
 &\leq C z^2 \prod_{\substack{p \leq z \\ p \in P}} \frac{1}{(1 - g(p))^3} = \frac{C z^2}{V(z)}, \text{ что и требовалось.}
 \end{aligned}$$

Укажем некоторые приложения доказанных теорем. Нам потребуется одно вспомогательное утверждение.

Лемма 1 Пусть $z \geq 1$ — целое число, и пусть $H_z(x) = \sum_{\substack{d \leq x \\ (d, z) = 1}} \frac{\mu^2(d)}{\varphi(d)}$. Тогда при любом $x \geq 1$ справедлива оценка:

$$H_z(x) \geq \frac{\varphi(z)}{z} (L(x)).$$

Д-во Сведём сначала оценку $H_z(x)$, $z \geq 2$, к оценке $H_1(x)$. Для заданного z имеем:

$$\begin{aligned}
 H_1(x) &= \sum_{d \leq x} \frac{\mu^2(d)}{\varphi(d)} = \sum_{\delta|z} \sum_{\substack{d \leq x \\ (d, z) = \delta}} \frac{\mu^2(d)}{\varphi(d)} = \sum_{\delta|z} \sum_{\substack{\delta m \leq x \\ (m, z) = 1}} \frac{\mu^2(\delta m)}{\varphi(\delta m)} \\
 &= \sum_{\delta|z} \frac{\mu^2(\delta)}{\varphi(\delta)} \sum_{\substack{m \leq \frac{x}{\delta} \\ (m, z) = 1}} \frac{\mu^2(m)}{\varphi(m)} = \sum_{\delta|z} \frac{\mu^2(\delta)}{\varphi(\delta)} H_z\left(\frac{x}{\delta}\right) \leq \\
 &\leq H_z(x) \sum_{\delta|z} \frac{\mu^2(\delta)}{\varphi(\delta)} = H_z(x) \prod_{p|z} \left(1 + \frac{1}{p-1}\right) = \frac{z}{\varphi(z)} H_z(x), \\
 \text{откуда} \quad H_z(x) &\geq \frac{\varphi(z)}{z} H_1(x).
 \end{aligned}$$

Оценим теперь $H_1(x)$. Имеем:

$$\begin{aligned}
 H_1(x) &= \sum_{d \leq x} \frac{\mu^2(d)}{d} \prod_{p|d} \frac{1}{1 - \frac{1}{p}} = \sum_{d \leq x} \frac{\mu^2(d)}{d} \prod_{p|d} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) \\
 &= \sum_{d \leq x} \frac{\mu^2(d)}{d} \sum_{m|d} \frac{1}{m}, \text{ где, как и ранее,}
 \end{aligned}$$

запись $n|d^\infty$ означает, что все простые делители n встречаются среди простых делителей d (или, что то же, n делит d^N при достаточно большом N).

Всякое n , $1 \leq n \leq x$, единственным образом представляется в виде $n = dm$, где $\mu(d) \neq 0$, а $n|d^\infty$.

Значит,

$$H_1(x) = \sum_{d \leq x} \sum_{n|d^\infty} \frac{\mu^2(d)}{dm} \geq \sum_{n \leq x} \frac{1}{n}.$$

Если $1 \leq x < 2$, то

$$\sum_{n \leq x} \frac{1}{n} \equiv 1 = \varrho x + 1 - \varrho x > \varrho x + 1 - \varrho 2 > \varrho x + \frac{3}{10};$$

если же $x \geq 2$, то

$$\sum_{n \leq x} \frac{1}{n} = \sum_{1 \leq n \leq [x]} \frac{1}{n} \geq 1 + \int_1^{[x]} \frac{dn}{n} = 1 + \varrho \cdot [x] \geq$$

$$\geq 1 + \varrho(x-1) = 1 + \varrho x + \varrho(1 - \frac{1}{x}) \geq \varrho x + 1 + \varrho \frac{1}{2} =$$

$$= \varrho x + 1 - \varrho 2 > \varrho x + \frac{3}{10}.$$

Итак, $H_1(x) > \varrho x + \frac{3}{10}$

$$H_2(x) > \frac{\varphi(x)}{x} \left(\varrho x + \frac{3}{10} \right).$$

при любых $x \geq 1$, откуда и следует утверждение леммы.

Теорема 4 (неравенство Брука-Титзмарша). При любых x и y , $2 \leq y \leq x$, и любых целых q и a условиях $(a, q) = 1$, $1 \leq a < q \leq y^C$ (где $C > 1$ — достаточно большая постоянная) справедлива оценка:

$$\pi(x+y; q, a) - \pi(x; q, a) \leq \frac{2y}{\varphi(q)} \cdot \frac{1}{\varrho \frac{2y}{q}} \left\{ 1 + \frac{3\varrho \varrho \frac{2y}{q}}{\varrho \frac{2y}{q}} \right\}$$

Док-во. Как и при нахождении этой оценки методом решета Брука, возьмем

$$a_n = \begin{cases} 1, & \text{если } x < n \leq x+y, n \equiv a \pmod{q}, \\ 0, & \text{иначе,} \end{cases}$$

$\mathcal{P} = \mathbb{P}$ и $2 \leq z \leq \sqrt{x+y}$. Тогда

$\pi(x+y; q, a) - \pi(x; q, a) \in S(A, P, z)$, Для оценки про-
сварающей функции заметим, что $|A_d| = 0$ при $(q, d) > 1$
(убо сравнения $k \equiv a \pmod{q}$, $k \equiv 0 \pmod{d}$ ввиду
условия $(a, q) = 1$ не могут выполняться одновре-
менно). Если же $(q, d) = 1$, то в силу китайской
теоремы об остатках эти сравнения можно заме-
нить одним: $k \equiv b \pmod{qd}$, где $b = add$, $dd \equiv 1 \pmod{q}$.
В этом случае имеем:

$$|A_d| = \sum_{\substack{x < k \leq x+y \\ k \equiv a \pmod{q} \\ k \equiv 0 \pmod{d}}} 1 = \sum_{\substack{x < k \leq x+y \\ k \equiv b \pmod{qd}}} 1 =$$

$$= \left[\frac{x+y-b}{qd} \right] - \left[\frac{x-b}{qd} \right] = \frac{y}{qd} + \theta, \quad |\theta| \leq 1$$

Следовательно, можно положить $X = \frac{y}{q}$,

$$g(d) = \begin{cases} \frac{1}{d}, & \text{если } (q, d) = 1, \\ 0, & \text{иначе,} \end{cases}$$

так что $|A_d| = Xg(d) + \tau_d$, где $|\tau_d| \leq 1$ при $(q, d) = 1$

и $\tau_d = 0$ при $(q, d) > 1$. В силу теоремы 2
имеем:

$$S(A, P, z) \leq \frac{X}{G(z)} + z^2 = \frac{y}{q} \cdot \frac{1}{G(z)} + z^2,$$

$$\text{где } G(z) = \sum_{\substack{d|P(z) \\ d \leq z}} \mu^2(d) h(d),$$

$$h(p) = \frac{g(p)}{1-g(p)} = \begin{cases} \frac{1}{\varphi(p)}, & \text{если } p \nmid q, \\ 0, & \text{иначе} \end{cases}$$

Следовательно, в обозначениях леммы 1

$$G(z) = \sum_{\substack{d \leq z \\ (d, q) = 1}} \frac{\mu^2(d)}{\varphi(d)} = H_q(z) \geq \frac{\varphi(q)}{q} \left(\log z + \frac{3}{10} \right),$$

так что

$$S(A, \mathcal{D}, z) \leq \frac{y}{\varphi(q)} \cdot \frac{y}{q} \cdot \frac{1}{(qz + \frac{3}{10})} + z^2 = \frac{y}{\varphi(q)} \cdot \frac{1}{(qz + \frac{3}{10})} + z^2.$$

Положив $z = \frac{\sqrt{\frac{2y}{q}}}{e^{\frac{2y}{q}}}$, получим:

$$\begin{aligned} S(A, \mathcal{D}, z) &\leq \frac{y}{\varphi(q)} \cdot \frac{1}{\frac{1}{2} e^{\frac{2y}{q}} - e e^{\frac{2y}{q}} + \frac{3}{10}} + \frac{\frac{2y}{q}}{e^{\frac{2y}{q}}} \cdot \frac{1}{e^{\frac{2y}{q}}} \leq \\ &\leq \frac{\frac{2y}{q}}{\varphi(q)} \cdot \frac{1}{e^{\frac{2y}{q}}} \left\{ \frac{1}{1 - \frac{2ae^{\frac{2y}{q}} - \frac{3}{5}}{e^{\frac{2y}{q}}}} + \frac{1}{e^{\frac{2y}{q}}} \right\} < \\ &< \frac{\frac{2y}{q}}{\varphi(q)} \cdot \frac{1}{e^{\frac{2y}{q}}} \left\{ 1 + 3 \cdot \frac{e e^{\frac{2y}{q}}}{e^{\frac{2y}{q}}} \right\}, \end{aligned}$$

если только $\frac{2y}{q} \geq C_0$, где C_0 — достаточно большая абсолютная постоянная. (подсчет показывает, что можно положить $C_0 = 2,7 \cdot 10^6$).

Теорема доказана.

В ряде случаев весьма желательно иметь оценку величины $\Phi_q(x) = \sum_{n \leq x, (n, q) = 1} 1$, равномерно по параметрам q и x . Один из вариантов такой оценки дается следующей теоремой.

Теорема 5. Пусть $x \geq e^6$, q — целое число, наибольший простой делитель которого не превосходит x . Тогда $\Phi_q(x) < 7 \frac{\varphi(q)}{q} x$.

До-во. Пусть $\mathcal{P}$ — множество всех простых делителей q (так что $\mathcal{P} \subseteq [2, x]$). Беря произвольное z , $2 \leq z \leq x$, и полагая $P = \prod_{p|q, p \leq z} p$, для последовательности $a_n = \begin{cases} 1, & n \leq x \\ 0, & n > x. \end{cases}$ получим из теоремы 2:

$$\Phi_q(x) \leq \sum_{\substack{n \leq x \\ (n, P)=1}} 1 \leq \frac{x}{G(z)} + z^2, \quad \text{где } G(z) = \sum_{\substack{d \leq z \\ d|P}} \frac{\mu^2(d)}{\varphi(d)}$$

Если обозначить через Q произведение всех простых $p \leq z$, не делящих q , то сумму $G(z)$ можно записать в виде

$$G(z) = \sum_{\substack{d \leq z \\ (d, Q)=1}} \frac{\mu^2(d)}{\varphi(d)} = H_Q(z).$$

Согласно лемме 1,

$$H_Q(z) \geq \frac{\varphi(Q)}{Q} \ln z, \quad \text{так что}$$

$$\Phi_q(x) \leq \frac{x}{\ln z} \cdot \frac{Q}{\varphi(Q)} + z^2 = \frac{x}{\ln z} \prod_{\substack{p \leq z \\ p \nmid q}} \left(1 - \frac{1}{p}\right)^{-1} + z^2.$$

Но тогда

$$\frac{z}{\varphi(q)} \cdot \frac{\Phi_q(x)}{x} \leq \frac{q}{\varphi(q)} \left\{ \frac{1}{\ln z} \prod_{\substack{p \leq z \\ p \nmid q}} \left(1 - \frac{1}{p}\right)^{-1} + \frac{z^2}{x} \right\} =$$

$$= \frac{q}{\varphi(q)} \prod_{\substack{p \leq z \\ p \nmid q}} \left(1 - \frac{1}{p}\right)^{-1} \left\{ \frac{1}{\ln z} + \frac{z^2}{x} \prod_{\substack{p \leq z \\ p \nmid q}} \left(1 - \frac{1}{p}\right) \right\} \leq$$

$$\leq \prod_{p|q} \left(1 - \frac{1}{p}\right)^{-1} \prod_{p \nmid q, p \leq z} \left(1 - \frac{1}{p}\right)^{-1} \left\{ \frac{1}{\ln z} + \frac{z^2}{x} \right\} \leq$$

$$\leq \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \left(\frac{1}{\ln z} + \frac{z^2}{x} \right).$$

Согласно неравенству Росера - Шенфилда,

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \leq e^{\gamma}(\ln x) \left(1 + \frac{1}{2 \ln x}\right),$$

$$\text{и } \frac{q}{\varphi(q)} \cdot \frac{\Phi_q(x)}{x} \leq e^{\gamma}(\ln x) \left(\frac{1}{\ln z} + \frac{z^2}{x} \right) \left(1 + \frac{1}{2 \ln x}\right) =$$

$$= e^{\gamma} \left(\frac{\ln x}{\ln z} + \frac{z^2}{x} \ln x \right) \left(1 + \frac{1}{2 \ln x}\right).$$

Беря $z = x^{1/3}$, при $x \geq e^6$ получим искомое.