Известия вузов. Математика
2017, № 11, с. 60–67

http://kpfu.ru/science/nauchnye-izdaniya/ivrm/
e-mail: izvuz.matem@kpfu.ru

Ф.Ф. ШАРИФУЛЛИНА

О ГЛАДКОСТЕПЕННЫХ ЧИСЛАХ

Аннотация. Натуральное число n называется y-гладкостепенным, где y — некоторое положительное число, если все делители n, являющиеся степенью простого числа, не превосходят y. Через $\psi^*(x,y)$ обозначим функцию количества y-гладкостепенных чисел на отрезке $[0,x]$. В этой статье исследуем функцию $\psi^*(x,y)$ и гладкостепенные числа в целом. Получены формулы для нахождения значений функции количества гладкостепенных чисел для больших x и сравнительно небольших y, а также даны теоретические оценки этой функции и функции наибольшего гладкостепенного числа. Полученные результаты можно использовать в криптографии и теории чисел для оценки сходимости алгоритмов факторизации целых чисел.

Ключевые слова: гладкие числа, гладкостепенные числа, разложение чисел на простые сомножители, оценки для алгоритмов в криптографии, алгоритм факторизации Ленстры, $(p-1)$-метод Полларда, RSA.

УДК: 519.7

Введение

Пусть y — произвольное положительное число. Натуральное число n называется *y-гладким*, если все его простые делители не превосходят y. И n называется *y-гладкостепенным* (y-*power smooth*), если любой делитель n, являющийся степенью p^k простого числа p, удовлетворяет условию $p^k \leq y$.

Каждое y-гладкостепенное число является y-гладким. Обратное неверно и существуют y-гладкие числа, не являющиеся y-гладкостепенными. Например, 48 является 10-гладким, но не 10-гладкостепенным. Если не указано иное, гладкостепенное число означает y-гладкостепенность.

Обозначим через $\psi(x,y)$ функцию количества y-гладких чисел $n \leq x$, а через $\psi^*(x,y)$ — функцию, равную числу натуральных чисел $n \leq x$, являющихся y-гладкостепенными. Из вышесказанного следует, что $\psi^*(x,y) \leq \psi(x,y)$ для всех x, y.

Функция $\psi^*(x,y)$ играет существенную роль при выборе параметров метода факторизации Ленстры с использованием эллиптических кривых. Для сходимости метода Ленстры необходимо, чтобы размерность эллиптической кривой, используемой в методе, была y-гладкостепенным числом при x, равном меньшему множителю факторизуемого числа [1].

На данный момент существует множество формул и алгоритмов, вычисляющих значения функции количества гладких чисел, точно или приближенно [2], тогда как исследования функции количества гладкостепенных чисел найдено не было, за исключением статьи [3], а в приложениях ее значения обычно заменяют на $\psi(x,y)$. Например, расчеты ([4], с. 338)

Поступила 27.06.2016

сходимости процедуры факторизации целых чисел методом эллиптических кривых Ленстры выполнены с использованием функции $\psi(x,y)$, хотя должна была быть использована $\psi^*(x,y)$.

Между тем функции $\psi^*(x,y)$ и $\psi(x,y)$ ведут себя по-разному. На графике (рис. 1) даны значения функций $\psi(x,y)$ (верхняя линия) и $\psi^*(x,y)$ при $y=6$ и $x=6^k$, $k=1,2,3,4$:

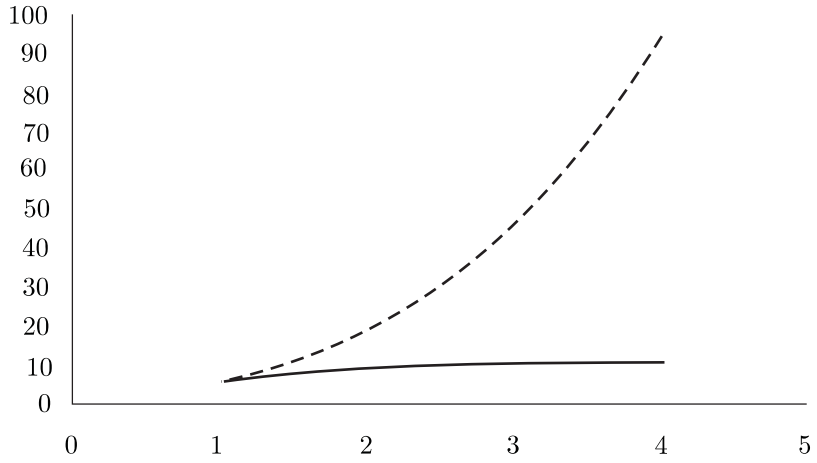

Рис. 1.

Как видно из графика, функция $\psi^*(x,y)$, начиная с некоторого x, остается постоянной. Это объясняется тем, что в случае функции $\psi^*(x,y)$ можно вести речь обо всех y-гладкостепенных числах, не ограничивая множество сверху числом x, в отличие от функции $\psi(x,y)$, так как для заданного y существует наибольшее y-гладкостепенное число.

Рассмотрим в каких случаях значения функции $\psi^*(x,y)$ могут быть заменены значениями $\psi(x,y)$, а в каких нет.

Значения функций $\psi(x,y)$ и $\psi^*(x,y)$ не сравнимы при $y << x$, к примеру если $y < \ln x$, то $\psi^*(x,y) \ll \psi(x,y)$. Пусть $x = 30000$, $y = \ln x$, тогда $\psi(x,y) = 483$, а $\psi^*(x,y) = 48$, для бóльших x картина не меняется.

С приближением y к x функция $\psi^*(x,y)$ приближается к $\psi(x,y)$. Но для больших x уже при $y > \sqrt{x}$ значения функций $\psi(x,y)$ и $\psi^*(x,y)$ довольно близки. К примеру $x = 10^8$, $y = \sqrt{x}$, тогда $(\psi(x,y) - \psi^*(x,y))\,/\psi(x,y) = 0.007$.

1. Функция $\psi^*(y)$

Пусть $p_1 = 2 < p_2 = 3 < p_3 < \cdots$ — последовательность всех простых чисел. Рассмотрим функцию $k(p,y) = \min\{t \in \mathbf{N} : p^t \geq y\}$, ее значения могут быть найдены по формуле $k(p,y) = \lceil \log_p y \rceil$, где $\lceil u \rceil$ — округление вверх.

Число всех y-гладкостепенных чисел обозначим через $\psi^*(y)$, а число всех простых чисел, не превышающих y через $\pi(y)$. Тогда любое гладкостепенное число имеет вид

$$p_1^{s_1} \cdot \ldots \cdot p_{\pi(y)}^{s_{\pi(y)}}, \tag{1}$$

где $0 \leq s_i < k(p_i,y)$, а $1 \leq i \leq \pi(y)$. Таким образом, когда s_i пробегают все свои значения получаем все y-гладкостепенные числа. Когда степени s_i принимают свои наибольшие значения $s_i = k(p_i,y) - 1 = \lceil \log_{p_i} y \rceil - 1 = \lfloor \log_{p_i} y \rfloor$ получаем *наибольшее гладкостепенное*

число

$$\mathrm{mps}(y) = p_1^{\lfloor \log_{p_1} y \rfloor} \cdot \ldots \cdot p_{\pi(y)}^{\lfloor \log_{p_{\pi(y)}} y \rfloor} = \prod_{i=1}^{\pi(y)} p_i^{\lfloor \log_{p_i} y \rfloor}. \tag{2}$$

Наибольшее гладкостепенное число не что иное как функция $M(B_1)$ ([5], с. 54), которая является ключевым параметром в $(p-1)$-методе Полларда как и k ([5], с. 90) из алгоритма Ленстры.

Значение функции $\psi^*(y)$ может быть найдено по формуле $\psi^*(y) = \prod\limits_{i=1}^{\pi(y)} k(p_i, y)$ или

$$\psi^*(y) = \prod_{i=1}^{\pi(y)} \lceil \log_{p_i} y \rceil. \tag{3}$$

Формула (3) может быть применима для нахождения значений функции $\psi^*(x, y)$, когда $x \geq \mathrm{mps}(y)$. Но при x, намного меньшем наибольшего гладкостепенного числа, эта формула не подходит.

2. Множество $s(x, y)$

Пусть $s(x, y)$ обозначает множество y-гладких чисел, не превышающих x, не являющихся y-гладкостепенными, а $\#s(x, y)$ — число элементов в этом множестве.

Пример 1. Имеем $s(100, 10) = \{16,\ 32,\ 48,\ 64,\ 80,\ 96,\ 27,\ 54,\ 81,\ 25,\ 50,\ 75,\ 100,\ 49,\ 98\}$.

Отсюда видно, что если $x \leq y^2$, то множество $s(x, y)$ состоит из кратных степеней p^k простых чисел $p \leq y$:

$$\#s(x, y) = \sum_{p \leq y} \left\lfloor \frac{x}{p^k} \right\rfloor, \quad k = k(p, y). \tag{4}$$

Если $x > y^2$, то эта формула должна быть скорректирована, так как, во-первых, не все кратные элементы p^k будут гладкими, и, во-вторых, к примеру, кратные произведения $p_i^{k(p_i,y)} \cdot p_j^{k(p_j,y)}$ будут учтены дважды, как кратные $p_i^{k(p_i,y)}$ и $p_j^{k(p_j,y)}$. Аналогично для троек, четверок и т. д.

Пример 2. Пусть $y = 10$, $x = 1000$. При $p = 2$ наименьшая степень 2, превышающая 10, есть 16. Отношение $\lfloor x/p^k \rfloor = \lfloor 1000/16 \rfloor = 62$, однако только 34 кратных из 62 будут 10-гладкими. Аналогично, для $p \in \{3,\ 5,\ 7\}$ такие кратные образуют множества, содержащие 25, 26, 16 элементов соответственно.

Поскольку пересечения этих множеств не пусты, то некоторые элементы оказались учтенными дважды. Все такие элементы имеют вид $p_i^{k_i} p_j^{k_j}$ для $p_i < p_j \leq y$ или являются y-гладкими кратными таких произведений.

В нашем примере будут дважды учтены следующие произведения:

$16 \cdot 27 = 432$ и $2 \cdot 16 \cdot 27 = 864$, $16 \cdot 25 = 400$ и $2 \cdot 16 \cdot 25 = 800$, $16 \cdot 49 = 784$, $25 \cdot 27 = 675$.

Подсчет числа таких элементов выполняется по формуле

$$\sum_{p_i < p_j \leq y} \left\lfloor \frac{x}{p_i^{k_i} \cdot p_j^{k_j}} \right\rfloor = \left\lfloor \frac{1000}{2^4 \cdot 3^3} \right\rfloor + \left\lfloor \frac{1000}{2^4 \cdot 5^2} \right\rfloor + \left\lfloor \frac{1000}{2^4 \cdot 7^2} \right\rfloor + \left\lfloor \frac{1000}{3^3 \cdot 5^2} \right\rfloor + \left\lfloor \frac{1000}{3^3 \cdot 7^2} \right\rfloor + \left\lfloor \frac{1000}{5^2 \cdot 7^2} \right\rfloor =$$

$$= 2 + 2 + 1 + 1 + 0 + 0 = 6.$$

Таким образом, $\#S(1000, 10) = 34 + 25 + 26 + 16 - 6 = 95$.

3. Общая формула для вычисления мощности множества $s(x,y)$

Теорема. *Имеем*

$$\#s(x,y)=\sum_{p\le y}\psi\left(\left\lfloor\frac{x}{p^k}\right\rfloor,y\right)-\sum_{p_i<p_j\le y}\psi\left(\left\lfloor\frac{x}{p_i^{k_i}\cdot p_j^{k_j}}\right\rfloor,y\right)+$$
$$+\sum_{p_i<p_j<p_l\le y}\psi\left(\left\lfloor\frac{x}{p_i^{k_i}\cdot p_j^{k_j}\cdot p_l^{k_l}}\right\rfloor,y\right)-\sum_{p_i<p_j<p_l<p_t\le y}\psi\left(\left\lfloor\frac{x}{p_i^{k_i}\cdot p_j^{k_j}\cdot p_l^{k_l}\cdot p_t^{k_t}}\right\rfloor,y\right)+\cdots+$$
$$+(-1)^{\pi(y)-1}\psi\left(\left\lfloor\frac{x}{p_1^{k_1}\cdot\ldots\cdot p_{\pi(y)}^{k_{\pi(y)}}}\right\rfloor,y\right).\quad(5)$$

Доказательство. Обозначим i-е слагаемое в формуле (5) через s_i. Как было отмечено в начале раздела, множество $s(x,y)$ состоит из кратных степеней $p^{k(p,y)}$ простых чисел $p\le y$. Но для общего случая формула (4) должна быть скорректирована. Необходимо, чтобы все кратные числа были гладкими числами, а также учесть слагаемые встречающиеся несколько раз.

1) Слагаемые из второй суммы s_2 входят в s_1 дважды, как кратные первого и второго множителя. Поэтому необходимо вычесть s_2 из s_1.

2) Слагаемые из s_3 входят в s_1 трижды, а значит, их нужно вычесть дважды, но s_3 входит и в s_2, которое уже вычли. Кратность вхождения s_3 в s_2 можно вычислить по формуле $\binom{3}{2}=3$. Значит, уже вычли s_3 три раза, а должны были только два. Следовательно, s_3 необходимо прибавить еще раз.

3) Слагаемые из s_4 входят в s_1 четыре раза, в s_2 $\binom{4}{2}$ — шесть раз, в s_3 $\binom{4}{3}$ — четыре раза, $4-6+4=2$, значит, слагаемые из s_4 встречаются дважды. Вычтем его.

4) Рассмотрим общий случай. Пусть k-е слагаемое s_k входит в s_1 $\binom{k}{1}=k$ раз, в s_2 — $\binom{k}{2}$ раз, в s_3 — $\binom{k}{3}$ раз, …, в s_{k-1} — $\binom{k}{k-1}$ раз

$$\binom{k}{1}-\binom{k}{2}+\binom{k}{3}-\cdots+(-1)^{k-2}\binom{k}{k-1}=R.$$

Известно, что $\binom{n}{0}-\binom{n}{1}+\cdots+(-1)^n\binom{n}{n}=0$. Тогда

$$\binom{k}{0}-R+(-1)^n\binom{k}{k}=0,\quad R=\binom{k}{0}+(-1)^k\binom{k}{k}=1+(-1)^k.$$

Если k четное, то $R=2$ и перед s_k надо ставить минус. Если k нечетное, то $R=0$ и перед s_k ставим плюс. □

Пример 3. Пусть $y=6$, $x=2000$. Точные значения функций ψ и ψ^* при этом равны 108 и 12 соответственно, а $\#s(x,y)=\psi-\psi^*=96$. Теперь найдем значение функции $\#s(x,y)$, используя формулу (5). Вычислим каждую сумму из правой части (5) отдельно:

$$\sum_{p\le y}\psi\left(\left\lfloor\frac{2000}{p^k}\right\rfloor,6\right)=\psi\left(\left\lfloor\frac{2000}{2^3}\right\rfloor,6\right)+\psi\left(\left\lfloor\frac{2000}{3^2}\right\rfloor,6\right)+\psi\left(\left\lfloor\frac{2000}{5^2}\right\rfloor,6\right)=$$
$$=\psi(250,6)+\psi(222,6)+\psi(80,6)=51+47+30=128,$$

$$\sum_{p_i<p_j\le y}\psi\left(\left\lfloor\frac{2000}{p_i^{k_i}\cdot p_j^{k_j}}\right\rfloor,6\right)=\psi\left(\left\lfloor\frac{2000}{2^3\cdot3^2}\right\rfloor,6\right)+\psi\left(\left\lfloor\frac{2000}{2^3\cdot5^2}\right\rfloor,6\right)+\psi\left(\left\lfloor\frac{2000}{3^2\cdot5^2}\right\rfloor,6\right)=$$

$$=\psi(27,6)+\psi(10,6)+\psi(8,6)=17+9+7=33,$$

$$\sum_{p_i<p_j<p_l\le y}\psi\left(\left\lfloor\frac{2000}{p_i^{k_i}\cdot p_j^{k_j}\cdot p_l^{k_l}}\right\rfloor,6\right)=\psi\left(\left\lfloor\frac{2000}{2^3\cdot3^2\cdot5^2}\right\rfloor,6\right)=\psi\left(\left\lfloor\frac{2000}{1800}\right\rfloor,6\right)=\psi(1,6)=1$$

$\#s(x,y)=128-33+1=96$.

4. Теоретические оценки

Оценим наибольшее y-гладкостепенное число $\mathrm{mps}(y)$. По формуле (2)

$$\mathrm{mps}(y)=\prod_{i=1}^{\pi(y)}p_i^{\lfloor\log_{p_i}y\rfloor}=\prod_{i=1}^{\pi(y)}p_i^{\log_{p_i}y-\{\log_{p_i}y\}}=\frac{\prod\limits_{i=1}^{\pi(y)}p_i^{\log_{p_i}y}}{\prod\limits_{i=1}^{\pi(y)}p_i^{\{\log_{p_i}y\}}}=\frac{y^{\pi(y)}}{\prod\limits_{i=1}^{\pi(y)}p_i^{\{\log_{p_i}y\}}}.$$

Оценим отдельно выражение в знаменателе получившейся дроби:

$$0\le\{\log_{p_i}y\}<1,\quad 1\le\prod_{i=1}^{\pi(y)}p_i^{\{\log_{p_i}y\}}<\prod_{i=1}^{\pi(y)}p_i.$$

Таким образом, $\frac{y^{\pi(y)}}{\prod\limits_{i=1}^{\pi(y)}p_i}<\frac{y^{\pi(y)}}{\prod\limits_{i=1}^{\pi(y)}p_i^{\{\log_{p_i}y\}}}\le y^{\pi(y)}$.

Прологарифмируем произведение $\prod\limits_{i=1}^{\pi(y)}p_i$: $\ln\prod\limits_{i=1}^{\pi(y)}p_i=\sum\limits_{i=1}^{\pi(y)}\ln p_i=\theta(\pi(y))$, где $\theta(x)$ — функция Чебышева ([6], с. 59). Имеем

$$\theta(x)\sim x\ \text{ при }\ x\to\infty\Longrightarrow\theta(\pi(y))\sim\pi(y),\quad y\to\infty,$$

$$\ln\prod_{i=1}^{\pi(y)}p_i\sim\pi(y),\quad\prod_{i=1}^{\pi(y)}p_i\sim\exp\{\pi(y)\}\ \text{ при }\ y\to\infty.$$

Конечная оценка имеет вид

$$\left(\frac{y}{e}\right)^{\pi(y)}<\mathrm{mps}(y)\le y^{\pi(y)}.\tag{6}$$

Здесь оценка снизу действительна при $y\to\infty$. Таким образом, для $x>y^{\pi(y)}$ точное значение функции $\psi^*(x,y)$ может быть найдено по формуле (3).

Согласно асимптотическому закону распределения простых чисел ([7], с. 11) $\pi(y)\sim\frac{y}{\ln y}$ при $y\to\infty$. Тогда условие $x>y^{\pi(y)}$ может быть переписано в виде $y<\ln x$.

Откуда следует, что при $y\to\infty$ и $y<\ln x$ функция $\psi^*(x,y)=\psi^*(y)=\prod\limits_{i=1}^{\pi(y)}\lceil\log_{p_i}y\rceil$. Формула не подходит для небольших значений y.

Для небольших значений y требуется другая оценка $\pi(y)$. К примеру подойдет оценка из ([4], с. 10): $\frac{y}{2\ln y}<\pi(y)<\frac{2y}{\ln y}$.

Таким образом, формула (3) верна для небольших $y<\frac{\ln x}{2}$.

Экспериментальные вычисления показали, что $\psi^*(x,y)$ может быть вычислена точно уже при $x > \exp\{1.01y\}$ или $y < \frac{100}{101}\ln x$. Теперь оценим функцию

$$\psi^*(y) = \prod_{i=1}^{\pi(y)} \lceil \log_{p_i} y \rceil = \prod_{i=1}^{\pi(y)} \lceil \frac{\ln y}{\ln p_i} \rceil \approx \prod_{i=1}^{\pi(y)} \frac{\ln y}{\ln p_i} = \frac{\prod \ln y}{\prod \ln p_i}.$$

В числителе все просто: $\prod\limits_{i=1}^{\pi(y)} \ln y = (\ln y)^{\pi(y)}$, а знаменатель прологарифмируем

$$\ln \prod_{i=1}^{\pi(y)} \ln p_i = \sum_{i=1}^{\pi(y)} \ln \ln p_i.$$

Используем асимптотическое равенство ([7], с. 28)

$$\sum_{p \le x} \frac{1}{p} = \ln \ln x + \gamma + O\left(\frac{1}{\ln x}\right) \quad \text{при} \quad x \to \infty,$$

где γ — постоянная Эйлера.

Будем считать, что $\ln \ln p_i \sim \sum\limits_{p \le p_i} \frac{1}{p}$, тогда

$$\sum_{i=1}^{\pi(y)} \ln \ln p_i = \sum_{i=1}^{\pi(y)} \sum_{p \le p_i} \frac{1}{p} = \frac{1}{2} + \left(\frac{1}{2} + \frac{1}{3}\right) + \cdots + \left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p_{\pi(y)}}\right) =$$

$$= \frac{\pi(y)}{2} + \frac{\pi(y)-1}{3} + \cdots + \frac{1}{p_{\pi(y)}} = \sum_{i=1}^{\pi(y)} \frac{\pi(y)-i+1}{p_i} =$$

$$= (\pi(y)+1) \sum_{i=1}^{\pi(y)} \frac{1}{p_i} - \sum_{i=1}^{\pi(y)} \frac{i}{p_i} \approx (\pi(y)+1)\ln\ln\pi(y) - \frac{\pi(y)}{\ln \pi(y)}.$$

Оценка второй суммы получена экспериментально.

Таким образом,

$$\psi^*(y) \approx \frac{(\ln y)^{\pi(y)}}{\exp\left\{\left(\pi(y)+1\right)\ln\ln\pi(y) - \frac{\pi(y)}{\ln\pi(y)}\right\}}.$$

5. Анализ случая $y < \ln x$

Наша задача в этом разделе определить множество чисел, для которых функция $\psi^*(x,y)$ может быть вычислена точно с использованием формулы (3).

Знаем все гладкостепенные числа (1) для фиксированного y, знаем их количество (3), но не знаем сколько их до x, если $\mathrm{mps}(y) > x$, т. е. в каком порядке они располагаются. Но на самом деле знаем, как располагаются последние p_k гладкостепенных числа (p_k — наибольшее простое число, не превосходящее y). Если всего гладкостепенных чисел $\psi^*(y)$ и $\mathrm{mps}(y) = p_1^{r_1} p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}$ — наибольшее гладкостепенное число, то

число	его номер
$p_1^{r_1}p_2^{r_2}\cdot\ldots\cdot p_{k-1}^{r_{k-1}}p_k^{r_k}$	$\psi^*(y)$
$p_1^{r_1-1}p_2^{r_2}\cdot\ldots\cdot p_{k-1}^{r_{k-1}}p_k^{r_k}$	$\psi^*(y)-1$
$p_1^{r_1}p_2^{r_2-1}\cdot\ldots\cdot p_{k-1}^{r_{k-1}}p_k^{r_k}$	$\psi^*(y)-2$
$\vdots$	$\vdots$
$p_1^{r_1}p_2^{r_2}\cdot\ldots\cdot p_{k-1}^{r_{k-1}-1}p_k^{r_k}$	$\psi^*(y)-p_k+1$
$p_1^{r_1}p_2^{r_2}\cdot\ldots\cdot p_{k-1}^{r_{k-1}}p_k^{r_k-1}$	$\psi^*(y)-p_k$

Теперь достаточно, чтобы $x > \frac{\mathrm{mps}(y)}{p_k}$. Найдя i такое, что $\frac{\mathrm{mps}(y)}{p_{i+1}} < x < \frac{\mathrm{mps}(y)}{p_i}$, имеем $\psi^*(x,y) = \psi^*(y) - i - 1$. По меньшей мере для $y \le 100000$ значение функции $\psi^*(x,y)$ может быть вычислено точно уже при $x > \exp\{1.01y\}$ или $y < \frac{100}{101}\ln x$.

Пример 4. Найдем $\psi^*(x,y)$ количество y-гладкостепенных чисел, не превосходящих x для $x = 10^{300}$, а $y = 600$. Для вычислений используем программу Вольфрам математика.

Если $y = 600$, то $\pi(y) = 109$, а 109-м простым числом является 599. Найдем наибольшее гладкостепенное число

$$\mathrm{mps}(600) = 2^{\lfloor \log_2 600\rfloor}\cdot\ldots\cdot 599^{\lfloor \log_{599} 600\rfloor} \approx 8.5 * 10^{257}.$$

Наибольшее гладкостепенное число меньше x, а значит, можем воспользоваться формулой (3):

$$\psi^*(10^{300},600) = \prod_{i=1}^{109}\lceil \log_{p_i} 600\rceil = 295717532021241354781150923750113280.$$

Пример 5. Пусть $y = 200$, $x = \exp\{202\} \approx 5.3 * 10^{87}$, тогда $p_k = 199$, а $\mathrm{mps}(y) \approx 3.4 * 10^{89}$, $x < \mathrm{mps}(y)$, но $\frac{\mathrm{mps}(y)}{p_k} \approx 1.7 * 10^{87} < x$, причем $\frac{\mathrm{mps}(y)}{67} < x < \frac{\mathrm{mps}(y)}{61}$, где $61 = p_{18}$, $\psi^*(y) = 4749890231992320$, а значит, $\psi^*(x,y) = \psi^*(y) - 18 - 1 = 4749890231992301$.

6. Заключение

Доказана формула для нахождения мощности множества всех гладких, но не гладкостепенных чисел. Таким образом, имея формулу для нахождения значений функции $\psi(x,y)$, можем найти и значения $\psi^*(x,y)$. Для больших x и y формула становится громоздкой.

Получены простые в вычислении формулы для нахождения значений функции количества гладкостепенных чисел для больших x и сравнительно небольших $y < \ln x$, а также даны теоретические оценки этой функции и функции наибольшего гладкостепенного числа $\mathrm{mps}(y)$. Установлена связь функции $\mathrm{mps}(y)$ с алгоритмом Ленстры и $(p-1)$-методом Полларда.

Дальнейшей задачей для себя ставим нахождение алгоритма или формулы для вычисления приближенного значения $\psi^*(x,y)$ для случая $\ln x < y < \sqrt{x}$, так как в этом случае значения функции $\psi^*(x,y)$ не могут быть заменены значениями $\psi(x,y)$.

Литература

[1] Lenstra H.W. jr. *Factoring integers whith elliptic curves*, Ann. Math. **126** (2), 649–673 (1987).

[2] Ishmukhametov Sh.T., Sharifullina F.F. *An algorithm for counting smooth integers*, Lobachevskii J. Math. **37** (2) 128–137 (2016).

[3] Sharifullina F.F., Ishmukhametov Sh.T. *About powersmooth numbers*, Reseach J. Appl. Sci. **10** (8), 381–384 (2015).
[4] Crandall R., Pomerance C. *Prime numbers*: *a computational perspective* (Springer-Verlag, Berlin, 2005).
[5] Ишмухаметов Ш.Т. *Методы факторизации натуральных чисел* (Казанск. ун-т, Казань, 2011).
[6] Нестеренко Ю.В. *Теория чисел* (Академия, М., 2008).
[7] Прахар К. *Распределение простых чисел* (Мир, М., 1967).

Ф.Ф. Шарифуллина

Казанский федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,

e-mail: farida.f.sharifullina@mail.ru

F.F. Sharifullina

On power smooth numbers

Abstract. A natural number n is called the y-power smooth for some positive number y if every prime power dividing n is bounded from above by the number y. Let us denote by $\psi^*(x, y)$ the amount of y-power smooth integers in the range from 0 to x. In this paper we investigate the function $\psi^*(x, y)$ and y-power smooth numbers in general. We derive formulas for finding exact calculation of $\psi^*(x, y)$ for large x and relatively small y, and give theoretical estimates for this function and for function of the greatest powersmooth number. This results can be used in the cryptography and number theory to estimate the convergence of the factorization algorithms.

Keywords: smooth integers, powersmooth integers, factorization, estimates for cryptographic algorithms, Lenstra elliptic curve factorization method, Pollard's $(p-1)$-factorization algorithm, RSA.

F.F. Sharifullina

Kazan Federal University,
18 Kremlyovskaya str., Kazan, 420008 Russia,

e-mail: farida.f.sharifullina@mail.ru