Research Journal of Applied Sciences 10 (8): 381-384, 2015
ISSN: 1815-932X

About Power Smooth Numbers

Farida F. Sharifullina and Shamil T. Ishmukhametov
Kazan (Volga Region) Federal University, Kremlevskaya Street 18, Kazan, Russia

Abstract: A positive integer n is called the y-smooth for some positive number y if all prime divisors n are bounded above by the number y. A natural number n is called the y-power smooth if every prime power dividing n is bounded above by the number y. In order to assess the cryptosecurity of some algorithms with public-key encryption such as the known method RSA, it is necessary to be able to calculate the function concerning the number of smooth and power smooth numbers within the set numeric intervals. Each y power smooth integer n is also an y-smooth but the reverse is not true. Let's denote by $\psi(x, y)$ the amount of y-smooth integers in the range from 0 to x and by $\psi^*(x, y)$ the amount of y-power smooth numbers ranging from 0 to x. The definition implies that $\psi^*(x, y) \leq \psi(x, y)$. In the scientific literature, one may meet a large number of publications devoted to the algorithm for calculating or approximating the function $\psi(x, y)$. However, the publications by the function $\psi^*(x, y)$ are almost absent. At large x and y the values of these functions are similar, however for large x and small y the values of $\psi(x, y)$ and $\psi^*(x, y)$ are significantly different. In this study, we give an overview of algorithms for calculating the amount of smooth and power smooth numbers at predetermined intervals and show our own results and observations.

Key words: Smooth numbers, power-smooth numbers, convergence, estimate for cryptographic algorithms, RSA

INTRODUCTION

Let y is a positive number. A positive integer n is called y-smooth if any prime divisor p of the number n satisfies the term $p \leq y$. A natural number n is called a power smooth one if any divisor of n which is the degree of p^k for a prime number p, satisfies the term $p^k \leq y$.

Each y-power smooth number is y-smooth one. The converse is not true and there are y-smooth numbers which are not y-power smooth. For example, 16 is a 10-smooth but not 10-power smooth.

We denote by $\psi(x, y)$ the function, equal to the set of natural numbers not exceeding x which are y-smooth and through $\psi^*(x, y)$ function, equal to the set of natural numbers $n \leq x$ which are power smooth ones. From the above, it follows that $\psi^*(x, y) \leq \psi(x, y)$ for all x, y. The smooth and power smooth numbers play an important role in number theory and cryptography and are used to evaluate the convergence of various theoretic number algorithms (Bernstein, 1995, 1998; De Bruijn, 1966; Hildebrand, 1986).

In Crandall and Pomerance (2005), Tenenbaum (1995) and Ishmukhametov (2014), one can find a necessary supporting material. In Hunter and Sorenson (1987), Hildebrand (1986), Hildebrand and Tenenbaum (1993), Hunter and Sorrenson (1997) and Parcel and Sorenson (2006) different algorithms are considered for the approximate computation of the function $\psi(x, y)$. The study describes one of the applications concerning the concepts of smoothness for the development of a fast factorization algorithm on elliptic curves (Amer *et al*., 1992).

Smooth numbers play an important role for the assessment of convergence concerning many theoretic number algorithms. Let's discuss the application of the smoothness concept in the following studies.

SMOOTH NUMBERS

Smooth numbers play an important role in assessing the convergence of the known factorization algorithms as the Number Field Sieve (NFS) and the Quadratic Sieve (QS) Method. More specifically, on the basis of these both methods the search procedure of y-smooth numbers is developed where y is the upper border of the base numerical factor. NFS Method is more efficient one because using the algebraic number fields the procedure of smooth numbers search may be more effective. When the required number of y-smooth numbers is found, a system of linear algebraic equations is developed with the coefficients of $F_2 = \{0, 1\}$ plurality and its solution provides the desired divider of a factorisable number.

The study of the smooth numbers distribution allows us to provide, the convergence assessment of NFS and QS methods to specify an upper limit for a solution search period.

Corresponding Author: Farida F. Sharifullina, Kazan (Volga Region) Federal University, Kremlevskaya Street 18, Kazan, Russia

Other applications of the concept of smoothness are in the number theory and other branches of mathematics. A detailed review of the applications concerning the concept of smoothness may be found in the review articles written by Granville (1989, 2004).

It should be noted that the concept of smoothness was studied by various mathematicians and a lot of different approximate formulas was found for the calculation of the function $\psi(x, y)$.

POWER SMOOTH NUMBERS

Power-smooth numbers also play an important role in number theory and cryptography but they were studied much less. It should be noted, first of all the use of power smooth numbers to assess such factorization algorithms as (p-1) Pollard Method, (p + 1) Williams Method and most importantly, the method of Lenstra the Elliptic Curves Method (ECM). All of these methods are based on the properties of number smoothness from the environment of a factorisable number dividers.

The latter method is the only subexponential method in this group, the rate of convergence of which determines the smallest divisor of a factorisable number. This allows the use of this method in cases when other methods, including NFS and QS are useless. For example, the full expansion of the 10th Fermat number became possible only due to ECM Method.

Since, there are no direct algorithms to compute the function $\psi^*(x, y)$ now a days, then at the assessment of these methods convergence the algorithms are considered for the estimation of $\psi(x, y)$ function which gives inaccurate assessments for assessing the ECM Method and similar methods. Moreover, the procedure of the 1st and 2nd Method stages selection is also not effective because of errors in the evaluation of power smooth numbers distribution. Therefore, the problem of finding the estimates for the function $\psi^*(x, y)$ plays an important role in the analysis of factoring algorithms.

FORMULAE FOR THE CALCULATION OF SMOOTH NUMBERS FUNCTION

The exact value of the function $\psi(x, y)$ may be found using the recurrent formula which is called the Buchstab's identity (Tenenbaum, 1995):

$$\psi(x,p_k) = \sum_{0\le i\le t_k} \psi\left(\frac{x}{p_k^i}, p_{k-1}\right) \quad (1)$$

Where:

t_k = $[\ln x/\ln p_k]$, $k>1$

p_k = Denotes e simple number

The values x and y in the arguments of the function $\psi(x, y)$ reach thousands of bits for modern applications. So, it is not possible to calculate the exact value according to Eq. 1. Therefore, it is necessary to use some approximations.

Today, there are many algorithms that allow to calculate the approximate value of the function $\psi(x, y)$. At the heart of many of them is well-known Dieckmann De Bruijn (1966) result:

$$\psi(x,y) \approx x \times \rho(u) \quad (2)$$

where, $u = \log_y x$ and ρ is Dieckmann de Bruijn function which is the solution of a differential equation:

$$u\rho'(u) + \rho(u-1) = 0 \quad (3)$$

with the original condition $\rho(u) = 1$ within the interval [0; 1]. The values of $\rho(u)$ function are tabulated with a high accuracy and its approximate value may be calculated according to Eq. 4:

$$\rho(u) \approx u^{-u} \quad (4)$$

This estimate is true for large y. Bruijn showed that the identity:

$$\psi(x, y) = x\,\rho(u)\{1+O(\log(u+1)/\log y)\},\ x = y^u$$

Is performed for $y>\exp(\log\log x)^{5/8+\varepsilon}$. Ennola formula may be used for $y<(\log x)^{1/2}$:

$$\psi(x,y) = \frac{1}{\pi(y)!}\prod\left(\frac{\log x}{\log p}\right)\left\{1+O\left(\frac{y^2}{\log x \log y}\right)\right\}$$

Hildebrand and Tenenbaum (1993) got a very strong result in giving the approximation of $\psi^*(x, y)$ for all $y\ge 2$.

As for the function $\psi(x, y)$, the calculation of its values was not performed and its importance in applications is usually replaced by $\psi(x, y)$. For example in Crandall and Pomerance (2005)'s monograph the convergence calculation procedure of integer factorization by the method of Lenstra elliptic curves was performed using the function $\psi(x, y)$, although $\psi^*(x, y)$ have to be used. This introduces a certain error in calculations.

As Table 1 shows the function $\psi(x, y)$ is growing much faster. Furthermore, the functions $\psi(x, y)$ and $\psi^*(x, y)$ have a significant difference. It is the sequence of all y-smooth numbers (with x limited on top) is infinite

Table 1: Here are the values of the functions $\psi(x, y)$ and $\psi^*(x, y)$ at $y = 25$

x	10^2	10^3	10^4	10^5
$\psi(x, y)$	275	1744	7866	28180
$\psi^*(x, y)$	204	780	1693	2466
$\psi^*(x, y)/\psi(x, y)$	0.7418	0.4472	0.2152	0.0875

whereas the sequence of power smooth numbers is finite. Let's consider the function $\psi^*(x, y)$ in more detail.

POWER SMOOTH NUMBERS

Let $p_1 = 2<p_2 = 3<...<p_n<$ is the sequence of all prime numbers. Let's denote the following via k(p, y) function:

$$k(p, y) = \min\{t\in N: p^t \geq y\}$$

Its values may be obtained according to the following formula:

$$k(p, y) = [\log_p y]$$

where [u] is the rounding up. The amount of all power smooth numbers we denote via $\psi^*(y)$ and the number of primes not exceeding y via $\pi(y)$. Then any power-smooth number looks as follows:

$$p_1^{s_1} \times ... \times p_{\pi(y)}^{s\pi(y)}$$

where:

$$0 \leq s_i < k(p_i, y), 1 \leq i \leq \pi(y)$$

Thus, when s_i run through all its values, we get all power-smooth numbers. The largest power-smooth number looks as follows:

$$p_1^{\left[\log_{p_1} y\right]} \times ... \times p_{\pi(y)}^{\left[\log_{p_{\pi(y)}} y\right]}$$

The values of the function $\psi^*(y)$ may be obtained according to the following formula:

$$\psi^*(y) = \prod_{i=1}^{\pi(y)} k(p_i, y)$$

or:

$$\psi^*(y) = \prod_{i=1}^{\pi(y)} \left[\log_{p_i} y\right]$$

To calculate the values of the function $\psi^*(x, y)$ at the values of x which are much smaller than the greatest power-smooth number the abovementioned formulae are inaccurate.

Let's consider the set of s(x, y) y-smooth numbers not exceeding x and which are not y power-smooth numbers. The number of elements for this set will be denoted via #s(x, y).

Example:

S(100, 10) = {16, 32, 48, 64, 80, 96, 27, 54, 81, 25, 50, 75, 100, 49, 98}

The example shows that if $x \leq y^2$, then the set s(x, y) consists of multiple degrees of p^k for the primes $p \leq y$:

$$\#s(x, y) = \sum_{p\leq y} \left[\frac{x}{p^k}\right], k = k(p, y)$$

If $x > y^2$, this formula must be adjusted as first of all not all multiple elements p^k will be smooth ones and secondly, the multiple products:

$$p_i^{k(p_i, y)} \times p_j^{k(p_j, y)}$$

will be counted twice as the multiples $p_i^{k(p_i, y)}$ and the multiples $p_j^{k(p_j, y)}$. Let's consider this situation by an example. Let x = 1000, y = 10. At $p_1 = 2$ the function $k(p_1, y) = 4$ and $p_1^{k(p_1, y)} = 16$. The relation $[x/p^k] = [1000/6] = 62$, although, only 34 multiples of 62 will be 10-smooth. Similarly for $p \in \{3, 5, 7\}$ such multiples form the sets containing 25, 26 and 16 elements, respectively.

While the intersections of these sets are not empty, some elements appeared to be counted twice. All of these elements have the following form:

$$p_i^{k(p_i, y)} \times p_j^{k(p_j, y)}$$

for $p_i < p_j \leq y$ or are y-smooth multiples of such products. In our example, the following products will be double-counted:

$$16\times27 = 432 \text{ and } 2\times16\times27 = 864$$
$$16\times25 = 400 \text{ and } 2\times16\times25 = 800$$
$$16\times49 = 784 \text{ and } 25\times27 = 675$$

The counting of such elements number is performed according to the following formula:

$$\sum_{p_i<p_j\leq y} \left[\frac{x}{p_i^{k(p_i, y)} \times p_j^{k(p_j, y)}}\right] = \left[\frac{1000}{2^4\times3^3}\right] + \left[\frac{1000}{2^4\times5^2}\right] + \left[\frac{1000}{2^4\times7^2}\right] + \left[\frac{1000}{3^3\times5^2}\right] + \left[\frac{1000}{3^3\times7^2}\right] + \left[\frac{1000}{5^2\times7^2}\right]$$
$$= 2+1+1+1+0+1 = 6$$

Thus, s#(1000, 10) = 34+25+26+16-6 = 95. Now, we are ready to put down a general formula for the calculation of #s(x, y):

$$\#s(x,y)=\sum_{p\le y}\psi\left(\left[\frac{x}{p^{k(p,y)}}\right],y\right)-\sum_{p_i<p_j\le y}\psi\left(\left[\frac{x}{p_i^{k(p_i,y)}\times p_j^{k(p_j,y)}}\right]y\right)+$$

$$\sum_{p_i\times p_j<p_l\times p_t\le y}\psi\left(\left[\frac{x}{p_i^{k(p_i,y)}\times p_j^{k(p_j,y)}\times p_l^{k(p_l,y)}\times p_t^{k(p_t,y)}}\right]y\right)$$

where the number of non-zero terms does not exceed $[\log_y x]-1$ and the absolute values of the terms are decreased rapidly, so the first term dominates all. Then, the function $\psi^*(x, y)$ may be found by the formula:

$$\psi^*(x,y)=\psi(x,y)-\#s(x,y)$$

These arguments show a non-trivial problem of calculating the function $\psi^*(x, y)$, the number of power smooth numbers. In order to obtain an approximating formula, this function is necessary to solve the problem of the function k(p, y) approximation and perform an error assessment.

CONCLUSION

The calculation of the function exact value for the set of power smooth numbers $\psi^*(x, y)$ at large values of x, y is a very time consuming task. Now a days, this issue is open and there are no satisfactory algorithms for its calculation. The replacement of the function $\psi^*(x, y)$ by the function $\psi(x, y)$ in the mathematical calculations is performed correctly enough without the estimation of an error occurring in this change. Therefore, the problem of algorithm development for the approximate calculation of the function $\psi^*(x, y)$ while maintaining accurate the asymptotic estimates is an important and an urgent task which has no solution to date.

ACKNOWLEDGEMENT

The research is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

REFERENCES

Amer, E., Sh.T. Ishmukhametov and R.G. Rubtsov, 1992. The of Lenstra factorization method convergence on elliptic curves, this collection.

Bernstein, D.J., 1995. Enumerating and counting smooth integers. Chapter 2, Ph.D Thesis, University of California at Berkeley.

Bernstein, D.J., 1998. Bounding Smooth Integers. In J.P. Buhler, Editor, Third International Algorithmic Number Theory Symposium, Portland, Springer, pp: 128-130.

Crandall, R. and C. Pomerance, 2005. The prime numbers: a computational perspective. Berlin: Springer-Verlag, pp: 604.

De Bruijn, N.G., 1966. On the number of positive integers ≤x and free of prime factors >y, Indagationes Mathematicae, 28: 239-247.

Granville, A., 1989. On positive integers ≤x with prime factors ≤t log x in: Number Theory and Applications (R.A. Mollin, Eds.), Kluver, pp: 40-422.

Granville, A., 2004. Smooth numbers: Computational number theory and beyond, Proc. MSRI workshop, pp: 268-363.

Hunter, S. and J. Sorenson, 1987. Approximating the number of integers free of large prime factors, Mathematics of Computation, 66 (220): 1729-1741.

Hildebrand, A., 1986. On the number of positive integers ≤x and free of prime factors >y. J. Num. Theory, 22 (3): 289-307.

Hildebrand, A. and G. Tenenbaum, 1993. On integers without large prime factors, J. de Theorie des Nombres de Bordeaux, 5: 1-74.

Hunter, S. and J. Sorrenson, 1997. Approximating the number of integers free of large primes. Math. Comp., 66 (220): 1729-1741.

Ishmukhametov, Sh.T., 2014. The methods of integer factoring [Text] Sh.T. Ishmuhametov (Eds.). LAP Lambert Academic Pub., pp: 256. ISBN: 978-3-659-17639-5.

Parcel, S. and J.P. Sorenson, 2006. Fast Bounds on the Distribution of Smooth Numbers, Proceedings of the 7th international conference on Algorithmic Number Theory ANTS'06, Springer-Verlag, Berlin, Germany, pp: 168-181.

Tenenbaum, G., 1995. Introduction to Analytic and Probabilistic Number Theory. Cambr. Stud. Advan. Mathem., Cambridge Univ. Press, 46: 448.