CS 681: Computational Number Theory and Algebra	Lecture 19: Smooth Numbers
Lecturer: Manindra Agrawal	Notes by: Arun Iyer
	September 20, 2005.

1 Smooth Numbers

Definition 1.1 *A number x is said to be y-smooth if all its prime factors are less than or equal to y.*

Example of Smooth Numbers :
1, 2, 4, 8, 16, 32, 64, 128, 256, 512, ... are 2-smooth
1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, ... are 3-smooth
1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, ... are 5-smooth
Smooth Numbers are used in Elliptic Curve Factoring, Quadratic Sieve and Number Field Sieve, the three most popular integer factoring algorithms. They are also used in index calculus method for discrete log problem. Before delving any further, we need to first get an idea of density of smooth numbers.

2 Density of Smooth Numbers

Let $\Psi(x, y) = \{m \leq x \,|\, m \; is \; y - smooth\}$
Let $\psi(x, y) = |\Psi(x, y)|$
Suppose m is y-smooth.
Then $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$
where $p_1, p_2, \dots, p_t$ are all primes less than or equal to y.

2.1 Upper Bound on the Density

One way to go about finding the upper bound is,

$$\begin{aligned} \psi(x, y) &= \prod_{i=1}^{t} (1 + \log_{p_i}(x)) \\ &\leq \prod_{i=1}^{t} (1 + \log_2(x)) \\ &= O((\log x)^t) \\ &= O((\log x)^{\frac{y}{\log y}}) \end{aligned}$$

Exercise 2.1 *Find a decent upper bound for $\psi(x, y)$.*

2.2 Lower Bound on the Density

The highest power of y that can divide into x is $\log_y(x)$. It is easily seen that, $\sum_{i=1}^{t} \alpha_i \geq \log_y(x) + t$. Therefore,

$$\begin{aligned}
\psi(x,y) &\geq \binom{\log_y(x)+t}{t} \\
&\geq \frac{t^{\log_y x}}{(\log_y x)!} \\
&= \Omega\left(\frac{t^{\log_y x}}{(\log_y x)^{\log_y x}}\right) \\
&= \Omega\left(\frac{x}{(\log_y x)^{2\log_y x}}\right)
\end{aligned}$$

3 References

1. Eric W. Weisstein. "Smooth Number." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/SmoothNumber.html