Notes on the second moment method, Erdős multiplication tables

January 25, 2011

1 Erdős multiplication table theorem

Suppose we form the $N \times N$ multiplication table, containing all the N^2 products ab, where $1 \leq a, b \leq N$. Not all these products will be distinct, since for example $ab = ba$; and, for example $2 \cdot 3 = 3 \times 2 = 6 \times 1 = 1 \times 6$. But we might hope that there are enough of them to where these products take up a "positive proportion" of the numbers up to N^2 as $N \to \infty$. That is, one might guess that:

Question. Let $m(N)$ denote the number of integers of the form ab, where $1 \leq a, b \leq N$. Does $\lim_{N\to\infty} m(N)/N^2$ exist, and is it equal to some non-zero (positive) constant?

P. Erdős showed that the answer is 'no'; that, in fact, $\lim_{N\to\infty} m(N)/N^2 = 0$. In other words, as N gets bigger and bigger, the set of products ab as above "eat up" a smaller and smaller proportion – tending to 0, in fact – of the integers up to N^2. What was innovative about Erdős's proof was that he did this using probabilistic arguments; and here we will trace through his proof.

2 Markov's inequality and Chebyshev's inequality

The main tools we will need are some elementary estimates in prime number theory, in combination with the following inequality:

Chebyshev's Inequality. Suppose that X is a random variable having finite variance σ^2 and expected value μ (i.e. $\mathbb{E}(X) = \mu$ and $V(X) = \sigma^2$). Then,

$$\mathbb{P}(|X - \mu| \geq t) \ \leq \ \sigma^2/t^2.$$

Another way to express the conclusion here is:

$$\mathbb{P}(|X - \mu| \geq t\sigma) \ \leq \ 1/t^2.$$

The proof of this inequality relies on *another* inequality called Markov's inequality, stated as follows:

Markov's Inequality. Suppose that $X \geq 0$ and has expected value $\mu > 0$. Then, for $t > 0$ we have

$$\mathbb{P}(X \ \geq \ t) \ \leq \ \mu/t.$$

2.1 Proof of Markov's inequality

We will prove it in the case where X is a continuous random variable having pdf $f(x)$; the discrete case can be handled similarly.

We begin by letting $1_{[t,\infty)}(x)$ denote the indicator function for the interval $[t, \infty)$, so that the function is 0 if $x < t$, and is 1 if $x \geq t$. Then, we observe that

$$1_{[t,\infty)}(x) \ \leq \ x/t, \text{ for } x > 0.$$

We have

$$\mathbb{P}(X \geq t) \ = \ \int_0^\infty 1_{[t,\infty)}(x) f(x) dx \ \leq \ \int_0^\infty x f(x)/t dx \ = \ \frac{\int_0^\infty x f(x) dx}{t} \ = \ \mu/t,$$

as claimed.

2.2 Proof of Chebyshev's inequality

We first note that if $\sigma^2 = 0$, then with probability 1 we have that $X = \mu$, since X is a continuous r.v. So we may assume $\sigma^2 > 0$.

Given X, let $Y = |X - \mu|^2$. Then, $Y \geq 0$ and $\mathbb{E}(Y) = \mathbb{E}(|X - \mu|^2) = \sigma^2 > 0$. It follows that

$$\mathbb{P}(|X - \mu| \geq t) \ = \ \mathbb{P}(Y \geq t^2) \ \leq \ \sigma^2/t^2,$$

where the last equality is a consequence of Markov's inequality.

3 Sums over prime numbers

We will also need the following well-known result in elementary prime number theory, which we will not bother to prove:

Theorem 1 *We have that*

$$\sum_{\substack{p \leq x \\ p \text{ prime}}} \frac{1}{p} \ = \ \log\log x + C + O(1/\log x),$$

where C is some constant.

Using the fact that

$$\sum_{\substack{p^a \geq 2,\ a \geq 2 \\ p \text{ prime}}} \frac{1}{p^a} \ = \ D,$$

for some constant $D > 0$, one can easily deduce from the above theorem that

Theorem 2 *We have that*

$$\sum_{\substack{p^a \leq x,\ a \geq 1 \\ p \text{ prime}}} \frac{1}{p^a} \ = \ \log\log x + E + O(1/\log x),$$

for some constant $E > 0$.

We will not bother to supply the proof of this.

One more fact we will need is given as follows:

Theorem 3

$$\sum_{\substack{p^a, q^b \leq x,\ a,b \geq 1 \\ p,q \text{ prime}}} \frac{1}{p^a q^b} \ \leq \ (\log\log x + E + O(1/\log x))^2.$$

Basically, we get this by squaring out the sum in Theorem 2.

4 The proof

Let $\Omega(n)$ denote the number of prime power divisors of n, and let $\omega(n)$ denote the number of prime divisors of n. So, for example, $\Omega(12) = 3$, because $2, 4$, and 3 are all the prime powers dividing 12; while, $\omega(12) = 2$, since 2 and 3 are the only prime divisors of 12.

It is an easy exercise to check that

$$\Omega(ab) \;=\; \Omega(a) + \Omega(b), \text{ for } a, b \geq 1.$$

A common way of expressing $\Omega(n)$ and $\omega(n)$ with sum notation is as follows:

$$\Omega(n) \;=\; \sum_{\substack{p^a | n \\ p \text{ prime}}} 1, \text{ and } \omega(n) \;=\; \sum_{\substack{p | n \\ p \text{ prime}}} 1.$$

The proof of Erdős's multiplication table theorem will amount to proving the following theorem.

Theorem 4 *For all but at most $o(N)$ of the integers $n \leq N$ we have that*

$$\log\log N - (\log\log N)^{2/3} \;<\; \Omega(n) \;<\; \log\log N + (\log\log N)^{2/3}. \qquad (1)$$

That is to say: For every $\varepsilon > 0$, there exists $N_0(\varepsilon) > 0$, such that if $N > N_0(\varepsilon)$ then (1) holds for at least $(1-\varepsilon)N$ of the integers in $\{1, 2, ..., N\}$.

Note. We get the same conclusion for the function $\omega(n)$.

Given this theorem, let us see how to prove Erdős's theorem: Basically, an easy consequence of this theorem is that all but at most $o(N^2)$ of the products ab, $1 \leq a, b \leq N$, have the property that (1) holds for *both* $n = a$ and $n = b$. Thus, all but at most $o(N^2)$ entries ab in the $N \times N$ multiplication table will satisfy

$$2\log\log N - 2(\log\log N)^{2/3} \;<\; \Omega(ab) \;<\; 2\log\log N + 2(\log\log N)^{2/3}.$$

But now how likely is it for a number $n \leq N^2$ to satisfy this inequality? Well, note that

$$\log\log(N^2) \;=\; \log(2\log N) \;=\; \log\log N + \log 2;$$

so, Theorem 4 is telling us that only $o(N^2)$ numbers $n \leq N^2$ have the property that $\Omega(n)$ is near $2 \log\log N$. What this means is that most pairs (a, b) lead to numbers ab with an atypically large number of prime power divisors, compared to most numbers of size at most N^2; and so, there can be only $o(N^2)$ numbers in the table, which proves Erdős's theorem.

4.1 Proof of Theorem 4

It remains, therefore, to prove Theorem 4. The idea is to use some probability: Basically, we let $X \leq N$ be a randomly selected number where every number up to N is chosen with equal probability $1/N$; and then we let $Y = \Omega(X)$. We have that

$$\begin{aligned} \mathbb{E}(Y) &= \sum_{x \leq N} \Omega(x) \mathbb{P}(X = x) = \frac{1}{N} \sum_{x \leq N} \sum_{\substack{p^a | x \\ p \text{ prime}}} 1 &= \frac{1}{N} \sum_{\substack{p^a \leq N \\ p \text{ prime}}} \sum_{\substack{x \leq N \\ p^a | x}} 1 \\ & &= \sum_{\substack{p^a \leq N \\ p \text{ prime}}} \frac{1}{N} \lfloor N/p^a \rfloor \end{aligned}$$

Now, $\lfloor N/p^a \rfloor = N/p^a - \delta_{p^a}$, where $0 \leq \delta_{p^a} < 1$; and so, we have that

$$\mathbb{E}(Y) = \sum_{\substack{p^a \leq N \\ p \text{ prime}}} \frac{1}{p^a} - \frac{1}{N} \sum_{\substack{p^a \leq N \\ p \text{ prime}}} \delta_{p^a}.$$

This last expression (the factor $1/N$ and sum multiplied together) clearly is bounded from above by 1; and so, $\mathbb{E}(Y) = \log\log N + O(1)$.

To compute the variance of Y, recall that

$$V(Y) = \mathbb{E}(Y^2) - \mathbb{E}(Y)^2 = \mathbb{E}(Y^2) - (\log\log N + O(1))^2.$$

For our purposes all we need is an upper bound here on $V(Y)$; and that is all we shall bother to prove: We have that

$$N\mathbb{E}(Y^2) = \sum_{x \leq N} \left(\sum_{\substack{p^a | x \\ p \text{ prime}}} 1 \right)^2 = \sum_{x \leq N} \sum_{\substack{p^a, q^b | x \\ p,q \text{ prime}}} 1 = \sum_{\substack{p^a, q^b \leq N \\ p,q \text{ prime}}} \sum_{\substack{x \leq N \\ p^a | x,\ q^b | x}} 1.$$

If p and q are distinct, then the number of $x \leq N$ divisible by p^a and q^b at the same time is just $\lfloor N/p^a q^b \rfloor$; on the other hand, if $p = q$ and $a < b$, then the count is just $\lfloor N/p^b \rfloor$. Let us consider the contribution of this second case (dropping the floors $\lfloor$ and $\rfloor$, since after all we are only interested in an upper bound):

$$\sum_{\substack{p^a, p^b \leq N \\ p \text{ prime}, \ a \leq b}} \frac{1}{p^b} \ \leq \ \sum_{\substack{p^b \leq N \\ p \text{ prime}, \ b \geq 2}} \frac{b}{p^b} \ \leq \ \sum_{\substack{p^b \leq N \\ p \text{ prime}, \ b \geq 2}} \frac{\log_2(p^b)}{p^b} \ = \ O(1).$$

The factor b in the numerator here accounts for the possibilities for a. The fact that we get $O(1)$ at the end is basically because those p^b, $b \geq 2$ are "quadratically thin" – there are at most $X^{1/2}$ such numbers in an interval $[X, 2X]$ for X large enough.

So, we get that

$$\mathbb{E}(Y^2) \ \leq \ O(1) + \sum_{\substack{p^a, q^b \leq N \\ p,q \text{ prime}, \ p \neq q}} \frac{1}{p^a q^b} \ \leq \ (\log\log N + O(1))^2,$$

by appealing to Theorem 3. It follows that

$$V(Y) \ \leq \ O(\log\log N);$$

and therefore, by Chebyshev's inequality, we have for any $c > 0$ that

$$\mathbb{P}(|Y - \mathbb{E}(Y)| \geq c(\log\log N)^{2/3}) \ \leq \ O(c^{-2}(\log\log N)^{-1/3}).$$

Since $\mathbb{E}(Y) = \log\log N + O(1)$ it is clear that this implies Theorem 4.