4 On the Scarcity of Simple Groups

P. Erdös

Denote by $f(x)$ the number of integers $n \leqslant x$ for which there is a simple group of order n. Dornhoff [2] proved that $f(x) = o(x)$ and Dornhoff and Spitznagel [3] proved that (c_1, c_2, ... denotes suitable positive absolute constants)

$$(1) \qquad f(x) < c_1 x \left[\frac{\log\log\log x}{\log\log x}\right]^{\frac{1}{2}}.$$

Denote by $f_1(x)$ the number of integers $n < x$ for which there is a non-cyclic simple group. We are going to prove the following sharper result.

Theorem 1.

$$f_1(x) < \frac{x}{\exp\left(\left(\frac{1}{\sqrt{2}} + o(1)\right)(\log x \log\log x)^{\frac{1}{2}}\right)}$$

Denote by $P(u)$ the greatest prime factor of u. Let $u_1 < u_2 < \ldots$ be the sequence of all integers which have a divisor $t_i \mid u_i$, $t_i > 1$, $t_i \equiv 1 \pmod{P(u_i)}$. Let $v_1 < v_2 < \ldots$ be the sequence of all integers such that for every $p \mid v_i$ there is a divisor $t_i(p)$ of v_i satisfying $t_i(p) \equiv 1 \pmod p$, $t_i(p) > 1$. Clearly every v is a u. Thus $U(x) \geqslant V(x)$ $\left(U(x) = \sum_{v_i < x} 1, V(x) = \sum_{u_i < x} 1 \right)$.

It follows from classical results on non-cyclic simple groups that if there is a non-cyclic simple group of order n then n is a v_i. For if $p^{\alpha} \mid n$, $p^{\alpha+1} \nmid n$ then the number of Sylow subgroups

$t(\alpha,p)$ of order p^{α} must be a divisor of n; further $t(\alpha,p) \equiv 1 \pmod p$ and if the group is non-cyclic we must have $t(\alpha,p) > 1$.

Instead of Theorem 1 we prove $\left(f_1(x) \leq V(x) \leq U(x)\right)$ and

$$(2) \qquad U(x) < \frac{x}{\exp\left(\left(\frac{1}{\sqrt{2}} + o(1)\right)(\log x \log\log x)^{1/2}\right)}$$

Denote by $\psi(x, y)$ the number of integers not exceeding x all whose prime factors are $\leq y$. Put $y^z = x$ and assume $z < 4y^{\frac{1}{2}} \log y$. A theorem of de Bruijn then states that [1]

$$(3) \qquad \psi(x, y) < c_2 x (\log x)^2 \exp(-z \log z - z \log\log z + c_3 z).$$

Now we are ready to prove (2). We split the integers $u_i < x$ into two classes. In the first class are the integers $u_i < x$ all whose prime factors are less than $\exp\left(\left(\frac{\log x \log\log x}{2}\right)^{\frac{1}{2}}\right) = I(x)$, and in the second class are other u's. $U_i(x)$ $(i = 1, 2)$ denotes the number of u's not exceeding x of the i-th class. By (3) we have by a simple computation $\left(z = \left(\frac{2 \log x}{\log\log x}\right)^{\frac{1}{2}}, \log z = \left(\frac{1}{2} + o(1)\right) \log\log x\right)$

$$(4) \qquad U_1(x) < \psi(x, I(x)) < x \exp\left(\left(-\frac{1}{\sqrt{2}} + o(1)\right) (\log x \log\log x)^{\frac{1}{2}}\right).$$

Now we estimate the number of u's of the second class $U_2(x)$. We evidently have

$$(5) \qquad \begin{aligned} U_2(x) &< \sum_{p \geq I(x)} \sum_{t=1}^{\infty} \left[\frac{x}{p(tp+1)}\right] < \sum_{p \geq I(x)} \sum_{t=1}^{x} \frac{x}{p(tp+1)} \\ &< x \sum_{p \geq I(x)} \frac{1}{p^2} \sum_{t=1}^{x} \frac{1}{t} < c_4 x \log x \sum_{p \geq I(x)} \frac{1}{p^2} < c_4 x \log x / I(x) \end{aligned}$$

Now since $U(x) = U_1(x) + U_2(x)$, (4) and (5) implies (2) and this completes the proof of Theorem 1.

With a little more trouble we can prove

Theorm 2. $U(x) = \dfrac{x}{\exp\left((1+o(1))\,(2 \log x \log\log x)^{\frac{1}{2}}\right)}$.

We only outline the proof of Theorem 2. It is easy to see that

$$U(x) < \sum_p \sum_t{}' \; \psi\left(\frac{x}{p(tp+1)}, p\right) \tag{6}$$

where the dash indicates that the summation is extended over all integers $t \geq 1$ for which all prime factors of $tp+1$ are less than or equal to p.

Using (3) we can deduce from (6) by a somewhat intricate computation that

$$f_1(x) < U(x) < \frac{x}{\exp\left((1+o(1)\;(2\log x\log\log x)^{\frac{1}{2}}\right)}\,. \tag{7}$$

To prove the opposite inequality we first observe that

$$U(x) > (1+o(1)) \sum_p \sum_t{}' \; \psi\left(\frac{x}{p(tp+1)}, p\right) \tag{8}$$

The proof of (8) is somewhat cumbersome and we suppress it. De Bruijn [1] proved that the right side of (3) also gives a lower bound for $\psi(x,y)$ (for a different value of c_3). From this fact and from (8) a simple computation gives

$$U(x) > \frac{x}{\exp\left((1+o(1))\;(2\log x\log\log x)^{\frac{1}{2}}\right)}\,. \tag{9}$$

Using (6) and (8) it perhaps should be possible to give an asymptotic formula for $U(x)$, but I have not succeeded in doing this.

I can prove that for $x > x_0$

$$f_1(x) \leqslant V(x) < \frac{x}{\exp\,(\sqrt{2}+c_5)\;(\log x\log\log x)^{\frac{1}{2}}}\,. \tag{10}$$

The proof of (10) is not quite simple and we suppress it. Further I can prove

$$V(x) > \frac{x}{\exp\,(c_6\,(\log x)^{\frac{1}{2}}\log\log x)}\,. \tag{11}$$

I do not know which of these estimates is closer to the true order of $V(x)$.

It seems likely that $f_1(x) < x^{1-c_7}$ but (11) shows that the method used in this paper cannot be used to improve our estimate for $f_1(x)$ very much.

REFERENCES

1. N. G. de Bruijn, *On the number of uncancelled elements in the sieve of Eratosthenes*, Indig. Math. 12 (1950), 247-250, see also *On the number of positive integers $\leq x$ and free of prime factors $> y$*, ibid., 13 (1951), 50-60.
2. L. Dornhoff, *Simple groups are scarce*, Proc. Amer. Math. Soc. 19 (1968), 692-696.
3. L. Dornhoff and E. L. Spitznagel Jr., *Density of finite simple group orders*, Math. Zeitschrift, 106 (1968), 175-177.