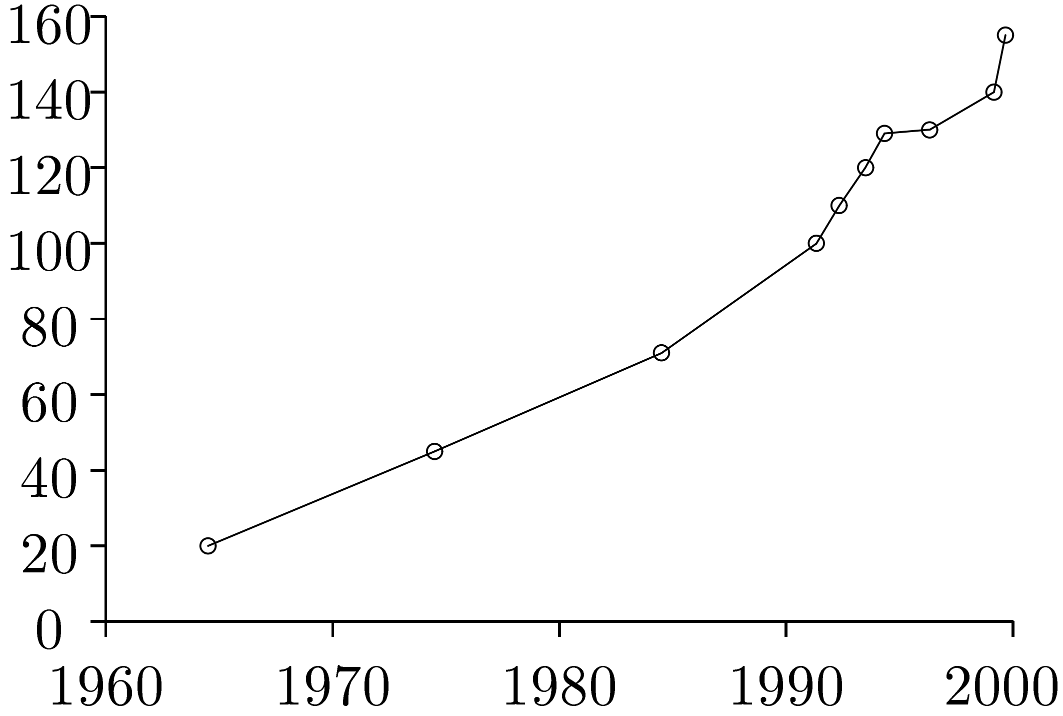
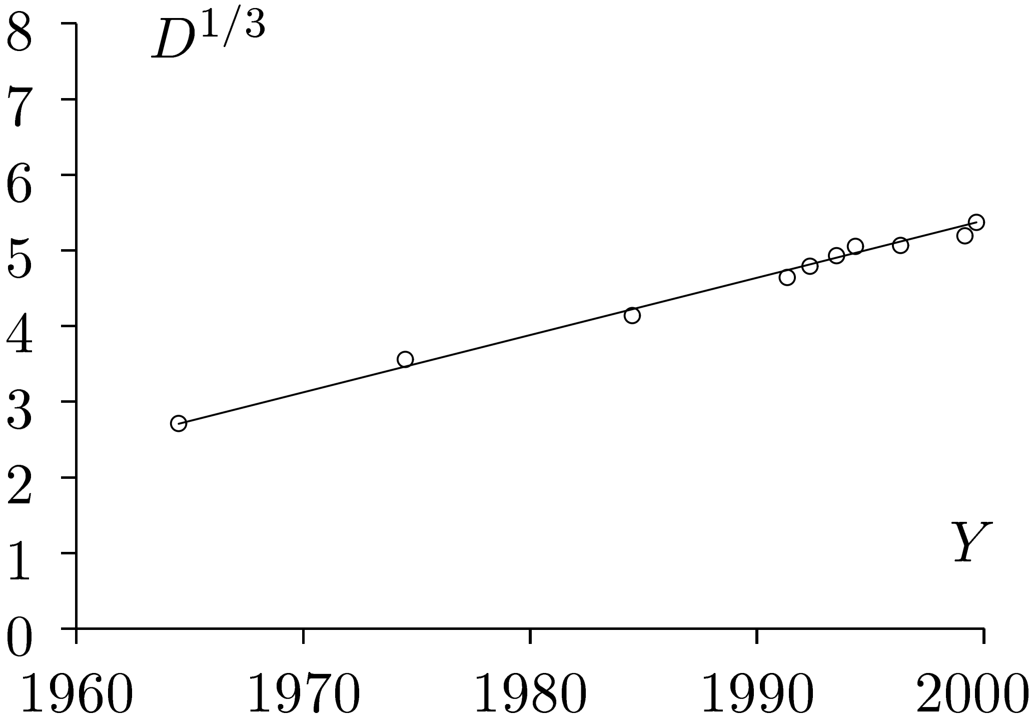
Historical Factoring Records



Size of "general" number factored versus year

The graph shows the size (in decimal digits) of the largest "general" number factored against the year it was done, from 1964 (20D) to 1999 (155D) (historical data from `www.rsa.com`).

Curve Fitting and Extrapolation



From the theoretical time bound for GNFS, assuming Moore's law, we expect $D^{1/3}$ to be roughly a linear function of time (we have assumed that $(\ln D)^{2/3}$ is roughly a constant). The graph shows $D^{1/3}$ versus year Y.

The straight line is

$$D^{1/3} = \frac{Y - 1928.6}{13.24}$$

and extrapolation, for what it is worth, gives $D = 309$ (i.e. 1024 bits) in the year $Y = 2018$.