Wie schwer ist Faktorisieren? Wie lange dauert das?

Prof. Dr. Dörte Haftendorn: Mathematik mit MuPAD 4.0, Update 4.01.09
http://haftendorn.uni-lueneburg.de www.mathematik-verstehen.de

reine Suche

```
spj:=60*60*24*366;
10^7
```

$$31622400$$

$$10000000$$

Sekunden pro Jahr

```
prfProJahr:=spj*10^10;
10^17
```

$$315360000000000000$$

$$1000000000000000000$$

Prüfungen pro Jahr

```
10.0^200/prfProJahr
```

$$3.170979198 \cdot 10^{182}$$

Das Beste, was es gibt

Beutelspacher Krypto in Theorie und Praxis S 51

```
f:=n->exp(1.9*ln(n)^(1/3)*ln(ln(n))^(2/3))
```

$$n \to e^{1.9 \cdot \sqrt[3]{\ln(n)} \cdot \ln(\ln(n))^{\frac{2}{3}}}$$

```
f(1.0*10^129)
```

$$3.59232668 \cdot 10^{17}$$

Umschreiben aud eine Funktion des Exponenten
(dort Vorzeichenfehler, hinten kein Minus-Exponent)

```
g:=s->float(E^(1.9*(s*ln(10)*(ln(s)+ln(ln(10)))^2)^(1/3)
));
ft(129), ft(300),ft(400);
```

$$s \to \mathrm{float}\left(E^{1.9 \cdot \sqrt[3]{s \cdot \ln(10) \cdot (\ln(s) + \ln(\ln(10)))^2}}\right)$$

$$3.59232668 \cdot 10^{17},\ 3.190247018 \cdot 10^{25},\ 7.728995454 \cdot 10^{28}$$

$$3.59232668 \cdot 10^{17},\ 3.190247018 \cdot 10^{25},\ 7.728995454 \cdot 10^{28}$$

Das ist also der nachgewiesen Wachstumstyp.

Mit diesem Algoritmus hat man mit 600 Computern in 1 Monat ein n mit 129 Stellen geknackt und dabei 1.6*10^17 Operationen benötigt.

Laufzeit = 1 Monat= 1/12 Jahr= c* g(129)

Daraus folgt c in Jahren.

```
c:=1/(12*g(129))
```

$$2.31975933 \cdot 10^{-19}$$

Wieviele FLOPS hatten diese Computer?

```
FlopsAlt:=12*1.6*10^17/spj;
12*1.6*10^17/spj/600
```

$$6.071645416 \cdot 10^{10}$$

$$101194090.3$$

Auffassung der 600 Computer als einen schnelleren mit 6*10^10 FlopsAlt.
Jeder einzelne der alten Computer hatte etwa 10^8 FLOPS

```
lauf:=(Flops,s)->c*FlopsAlt/Flops*g(s);
lauf(6.071645416*10^10,129)*12
```

$$(\text{Flops},\ s) \rightarrow \frac{c \cdot \text{FlopsAlt}}{\text{Flops}} \cdot g(s)$$

$$1.0$$

Es kommt die Ausgangssituation von 1 Monat Rechenzeit wieder heraus.

```
matrix([[129,300,400],
[lauf(FlopsAlt,129),lauf(FlopsAlt,300),lauf(FlopsAlt,400
)],
[lauf(10^12,129),lauf(10^12,300),lauf(10^12,400)],
[lauf(10^12,300)/lauf(10^12,129),
lauf(10^12,400)/lauf(10^12,129),
lauf(10^12,400)/lauf(10^12,300)]]);
```

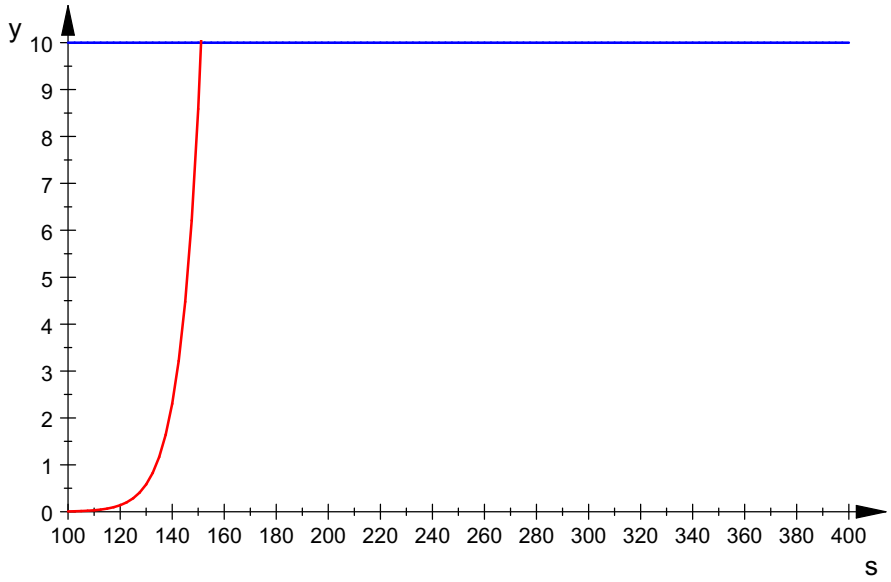
$$\begin{pmatrix} 129 & 300 & 400 \\ 0.08333333333 & 7400605.287 & 1.792940932 \cdot 10^{10} \\ 0.005059704513 & 449338.5116 & 1088610159.0 \\ 88807263.44 & 2.151529118 \cdot 10^{11} & 2422.694986 \end{pmatrix}$$

Zeile 2: Laufzeiten in Jahren mit dem alten Equipment.
Zeile 3: Laufzeiten in Jahren mit einem Rechner mit 10^12 FLOPS
statt altem Equipment 600 Rechner zu je 10^8 FLOPS.
Zeile 4 Laufzeit faktor bei 129->300 , 129->400 , 300->400

Fazit wenn man nun 1000 Rechner nehmen würde, die nochmal 100 mal schneller sind also 10^14 FLOPS, würde man für n mit 300 Stellen immernoch 4 Jahre brauchen.
Durch Ausweichen auf 400 Stellen erhöht sich dies auf 11000 Jahre.

Durch Ausweichen auf 400 Stellen erhöht sich dies auf 11000 Jahre.

```
plotfunc2d(10,lauf(10^a,s)/100 /* bis 100000*/,
s=100..400, a=8..15,
TimeBegin=8,TimeEnd=15,
ViewingBoxYRange=0..10, LegendVisible=FALSE)
```



animieren durch Anklicken!

Am Schieberegler kann man direkt ablesen welchen Zehnerexponenten man bei den FLOPS braucht, um 100 so schnellen Rechnern in 10 Jahren mit dem Faktorisieren fertig zu sein.