Lösungen, 9. 7. 2018

100.) Treffer-Positionen:

(5,9), (6,10), (7,11), (8,12), (9,13), (10,14), (11,15), (12,16)

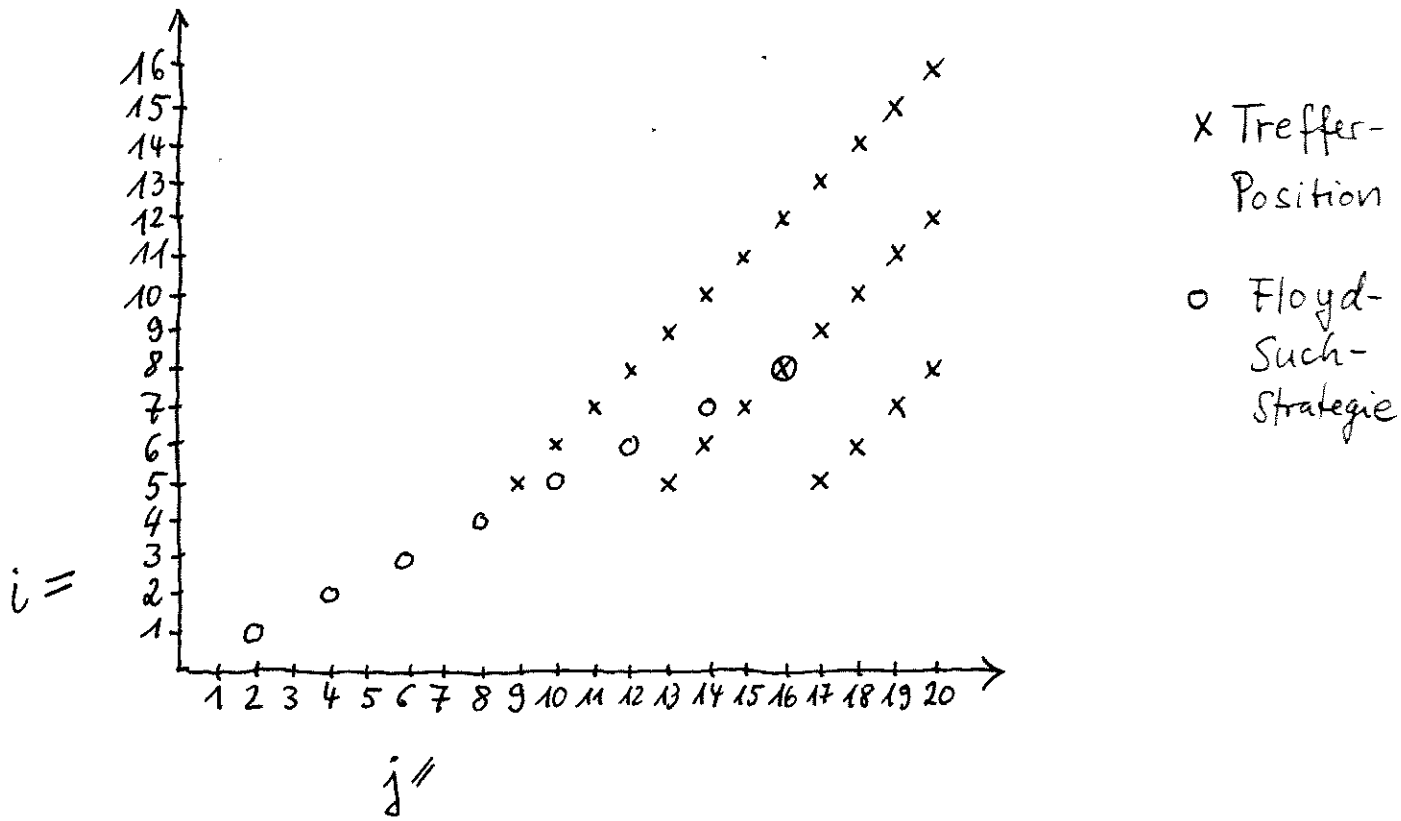
(13,17), (14,18), (15,19), (16,20)

Aber auch Folgende:

(5,13), (6,14), (7,15), (8,16), (9,17), (10,18), (11,19), (12,20)

Sowie:

(5,17), (6,18), (7,19), (8,20)



101.) $n = 2923$. Startwert für x ist

$\lceil \sqrt{n} \rceil = 55$ und für $z = x^2 - n = 102$.

x	z	Quadratzahl?
55	102	nein
56	213	nein
57	326	nein
58	441	ja: $441 = 21^2$, also $y = 21$

Ergibt die Faktoren $x - y = 58 - 21 = 37$

und $x + y = 58 + 21 = 79$.

102.) x durchläuft die Werte $\lceil \sqrt{n} \rceil$ bis $\frac{p+9}{2}$.

Bei $n \approx 2^{1000}$, $p \approx 2^{499}$ und $q \approx 2^{501}$ ist also der Bereich von $\approx 2^{500}$ bis $\approx \frac{2^{501} + 2^{499}}{2} \approx 2^{500} + 2^{498}$

Dies sind in der Größenordnung 2^{498} Schleifendurchläufe. Von „nahe beieinander" kann man nicht sprechen.

103.) Es ist $u = a^{\lceil \sqrt{n} \rceil} = 3^{12} = 18$, $v = \bar{a}^1 = 46$.

$\mathcal{L}_1 = \{(0,1), (1,18), (2,50), (3,78), (4,34), (5,64), (6,56),$
$(7,49), (8,60), (9,121), \boxed{(10,123)}, (11,22)\}$

$\mathcal{L}_2 = \{(0,11), (1,95), \boxed{(2,123)}, (3,41), (4,105), (5,35), (6,103),$
$(7,80), (8,118), (9,85), (10,74), (11,116)\}$

Also ist $x_1 = 10$, $x_2 = 2 \Rightarrow x = 10 \cdot 12 + 2$

$= \underline{\underline{122}}$

104.)

$a^1 \cdot y^1 = 40 \in M_3$

$a^2 \cdot y^2 = 7 \in M_1$

$a^3 \cdot y^2 = 14 \in M_1$

$a^4 \cdot y^2 = 28 \in M_2$

$a^4 \cdot y^3 = 29 \in M_2$ ← Dublette

$a^4 \cdot y^4 = 49 \in M_3$

$a^8 \cdot y^8 = 41 \in M_3$

$a^{16} \cdot y^{16} = 29 \in M_2$ ←

Somit $a^4 \cdot y^3 \equiv a^{16} y^{16} \pmod{59}$

$a^4 \cdot a^{3x} \equiv a^{16} \cdot a^{16x} \pmod{59}$

$a^{4+3x} \equiv a^{16+16x} \pmod{59}$

$4 + 3x \equiv 16 + 16x \pmod{58}$

$13x \equiv -12 \pmod{58}$

$x \equiv -12 \cdot 9 \pmod{58}$, da $9 = 13^{-1} \pmod{58}$

$x \equiv \underline{\underline{8}}$

Also $2^8 \equiv 20 \pmod{59}$

105.) Die 5-smooth numbers bis 25 sind:

2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25

Also $\Psi(25,5) = 15$

Approximation: $25 \cdot u^{-u} = 25 \cdot 2^{-2} = 6{,}25$

wobei $u = \frac{\log n}{\log B} = \frac{\log 25}{\log 5} = 2$.

Bei $B=10$ kommt nur die Primzahl 7 zur Faktorbasis $\{2,3,5\}$ hinzu. Die 7-smooth numbers sind obige, ergänzt um

7, 14, 21, also $\Psi(25,10) = \Psi(25,7) = 18$

Approximation: $25 \cdot u^{-u} \approx 15{,}65$

wobei $u \approx 1{,}4$

106.) Bei Faktorbasis $\{2\}$ muss eine Zahl z gefunden werden, die 2-smooth ist. Die Wahrscheinlichkeit dafür ist $\frac{7}{136}$. Daher muss im Erwartungswert $\frac{136}{7} \approx 19{,}4$ mal eine Zufallszahl gezogen werden.

Bei Faktorbasis $\{2,3\}$ brauchen wir 2 Zahlen, die 3-smooth sind. Dazu benötigt man im

Erwartungswert $\frac{136}{21} + \frac{136}{20} \approx 13{,}3$

Versuche.

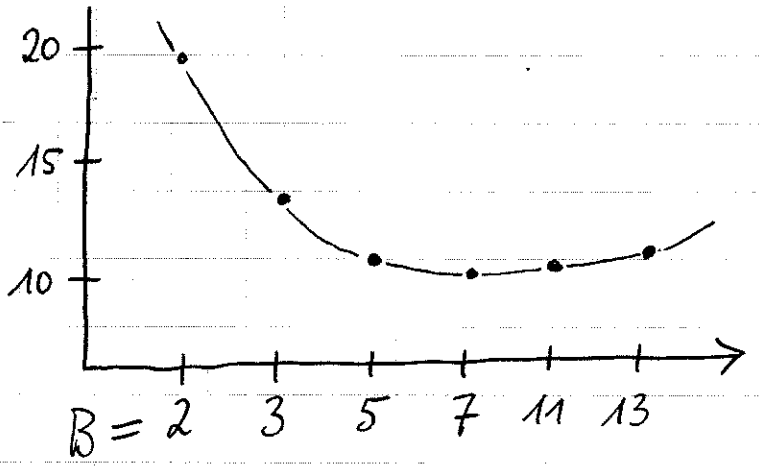
Die weiteren Erwartungswerte:

$\{2,3,5\}$: $\frac{136}{38} + \frac{136}{37} + \frac{136}{36} \approx 11{,}03$

$\{2,3,5,7\}$: $\frac{136}{53} + \frac{136}{52} + \frac{136}{51} + \frac{136}{50} \approx 10{,}57$

$\{2,3,5,7,11\}$: $\frac{136}{65} + \frac{136}{64} + \frac{136}{63} + \frac{136}{62} + \frac{136}{61} \approx 10{,}8$

$\{2,3,5,7,11,13\}$: $\frac{136}{75} + \frac{136}{74} + \frac{136}{73} + \frac{136}{72} + \frac{136}{71} + \frac{136}{70} \approx 11{,}26$



Der optimale B-Wert ist 7.

107.) Es ergeben sich die Kongruenzgleichungen

$10 \equiv 7x$ und $13 \equiv 2x + 3y \pmod{136}$

wobei x und y die diskreten Logarithmen von 2 und 3 sind. Mit Hilfe von $7^{-1} = 39$ ergibt sich $x = 118$. In die 2. Gleichung eingesetzt, mit Hilfe von $3^{-1} = 91$, ergibt sich $y = 107$.