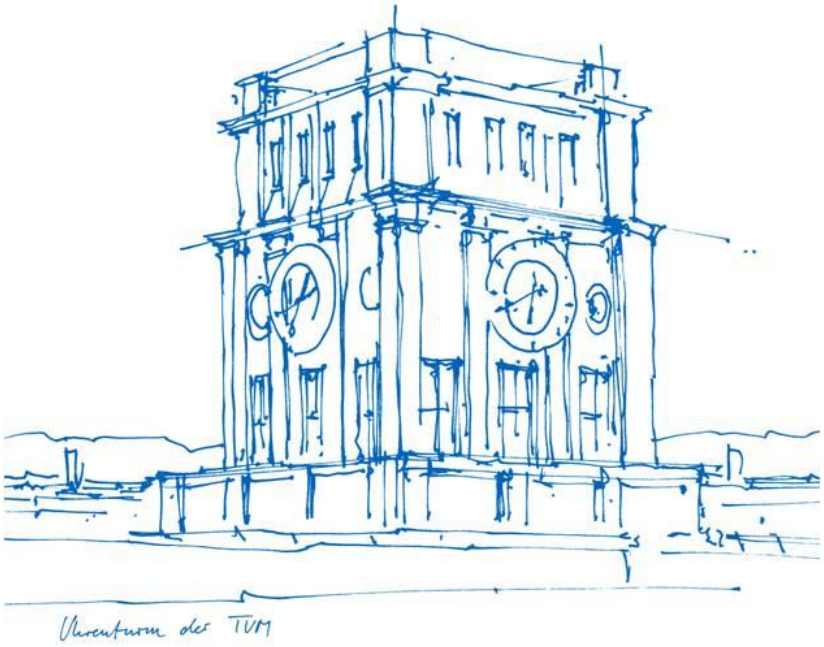
Aspekte der Systemnahen Programmierung bei der Spieleentwicklung

Projektaufgabe – 323: Berechnung von Primzahlen

Marcel Zurawka

Julius Krüger

Lars Hinnerk Grevsmühl



Mathematische Grundlagen

Die Wormell‘sche Formel

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2}\sum_{m=2}^{2^n}(-1)^2 \prod_{r=1}^{n}\left(1-r+\frac{m-1}{2}+\frac{1}{2}\sum_{x=2}^{m}(-1)^2 \prod_{a=2}^{x}\prod_{b=2}^{x}(x-ab)^2\right)^2$$

Zähler/Controller | Primzahltest

Mathematische Grundlagen

Die Wormell‘sche Formel

$$f(x) = \prod_{a=2}^{x} \prod_{b=2}^{x} (x - ab)^2$$

Primzahltest

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2} \sum_{m=2}^{2^n} (-1)^2 \prod_{r=1}^{n} \left(1 - r + \frac{m-1}{2} + \frac{1}{2} \sum_{x=2}^{m} (-1)^{2 \prod_{a=2}^{x} \prod_{b=2}^{x} (x-ab)^2} \right)^2$$

Mathematische Grundlagen

Die Wormell‘sche Formel

$$f(x) = \begin{cases} 0 & \text{wenn } n \text{ nicht prim} \\ N \in \mathbb{N} & \text{wenn } n \text{ prim} \end{cases}$$

Primzahltest

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2} \sum_{m=2}^{2^n} (-1)^2 \prod_{r=1}^{n} \left(1 - r + \frac{m-1}{2} + \frac{1}{2} \sum_{x=2}^{m} (-1)^{2 \prod_{a=2}^{x} \prod_{b=2}^{x} (x - ab)^2} \right)^2$$

Mathematische Grundlagen

Die Wormell‘sche Formel

$$g(m) = \sum_{x=2}^{m} \frac{1 + (-1)^{2^{f(x)}}}{2} = \frac{m-1}{2} + \frac{1}{2} \sum_{x=2}^{m} (-1)^{2^{f(x)}}$$

Zähler/Controller

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2} \sum_{m=2}^{2^n} (-1)^{2} \prod_{r=1}^{n} \left(1 - r + \frac{m-1}{2} + \frac{1}{2} \sum_{x=2}^{m} (-1)^{2} \prod_{a=2}^{x} \prod_{b=2}^{x} (x - ab)^2 \right)^2$$

Mathematische Grundlagen

Die Wormell‘sche Formel

$$g(m) = \sum_{x=2}^{m} \begin{cases} 0 & \text{wenn } f(x) = 0 \\ 1 & \text{wenn } f(x) \in \mathbb{N} \end{cases}$$

Zähler/Controller

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2} \sum_{m=2}^{2^n} (-1)^{2 \prod_{r=1}^{n} \left(1 - r + \frac{m-1}{2} + \frac{1}{2} \sum_{x=2}^{m} (-1)^2 \prod_{a=2}^{x} \prod_{b=2}^{x} (x - ab)^2 \right)^2}$$

Mathematische Grundlagen

Die Wormell‘sche Formel

$$h(m,n) = \prod_{r=1}^{n} (1 - r + g(m))^2$$

Zähler/Controller

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2} \sum_{m=2}^{2^n} (-1)^{2 \prod_{r=1}^{n} \left(1-r+\frac{m-1}{2}+\frac{1}{2} \sum_{x=2}^{m} (-1)^{2 \prod_{a=2}^{x} \prod_{b=2}^{x} (x-ab)^2} \right)^2}$$

Mathematische Grundlagen

Die Wormell‘sche Formel

$$h(m,n) = \begin{cases} 0 & \text{wenn } n > g(m) \\ N \in \mathbb{N} & \text{wenn } n \leq g(m) \end{cases}$$

Zähler/Controller

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2} \sum_{m=2}^{2^n} (-1)^{2 \prod_{r=1}^{n} \left(1 - r + \frac{m-1}{2} + \frac{1}{2} \sum_{x=2}^{m} (-1)^{2 \prod_{a=2}^{x} \prod_{b=2}^{x} (x-ab)^2} \right)^2}$$

Mathematische Grundlagen

Die Wormell‘sche Formel

$$i(n) = \sum_{m=2}^{2^n} \frac{1 + (-1)^{2^{h(m,n)}}}{2} = -\frac{1}{2} + 2^{n-1}\frac{1}{2}\sum_{m=2}^{2^n}(-1)^{2^{h(m,n)}}$$

Zähler/Controller

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2}\sum_{m=2}^{2^n}(-1)^2 \prod_{r=1}^{n}\left(1-r+\frac{m-1}{2}+\frac{1}{2}\sum_{x=2}^{m}(-1)^{2}\prod_{a=2}^{x}\prod_{b=2}^{x}(x-ab)^2\right)^2$$

Mathematische Grundlagen

Die Wormell‘sche Formel

$$i(n) = \sum_{m=2}^{2^n} \begin{cases} 0 & \text{wenn } h(m,n) = 0 \\ 1 & \text{wenn } h(m,n) \in \mathbb{N} \end{cases}$$

Zähler/Controller

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2} \sum_{m=2}^{2^n} (-1)^2 \prod_{r=1}^{n} \left(1 - r + \frac{m-1}{2} + \frac{1}{2} \sum_{x=2}^{m} (-1)^2 \prod_{a=2}^{x} \prod_{b=2}^{x} (x - ab)^2 \right)^2$$

Mathematische Grundlagen

Die Wormell‘sche Formel

$$p(n) = 2 + i(n) = p_n$$

Zähler/Controller

$$p_n = \frac{3}{2} + 2^{n-1} - \frac{1}{2} \sum_{m=2}^{2^n} (-1)^{2^{\prod_{r=1}^{n} \left(1-r+\frac{m-1}{2}+\frac{1}{2} \sum_{x=2}^{m} (-1)^{2} \prod_{a=2}^{x} \prod_{b=2}^{x} (x-ab)^2 \right)^2}}$$

Grenzen des Primzahltests

$$f(x) = \prod_{a=2}^{x} \prod_{b=2}^{x} (x - ab)^2$$

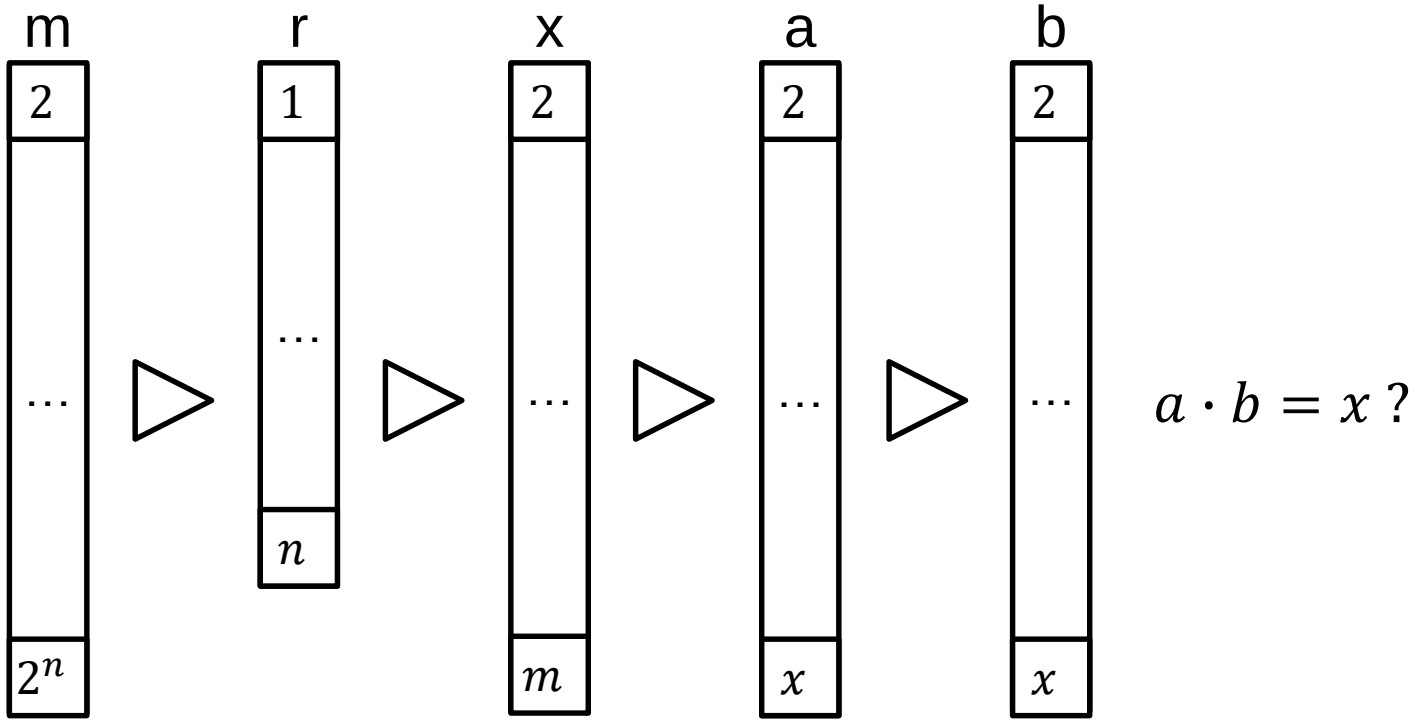
Primzahltest

Mögliche Optimierungen:

1. Abbruch nach gefundener Faktorisierung
2. Obergrenze für a bzw. b: x/2
3. Untergrenze für a: nicht Optimierbar
4. Untergrenzen für b:
   - unoptimiert
   - Annäherung an x/a über Zweierpotenzen
   - x/a

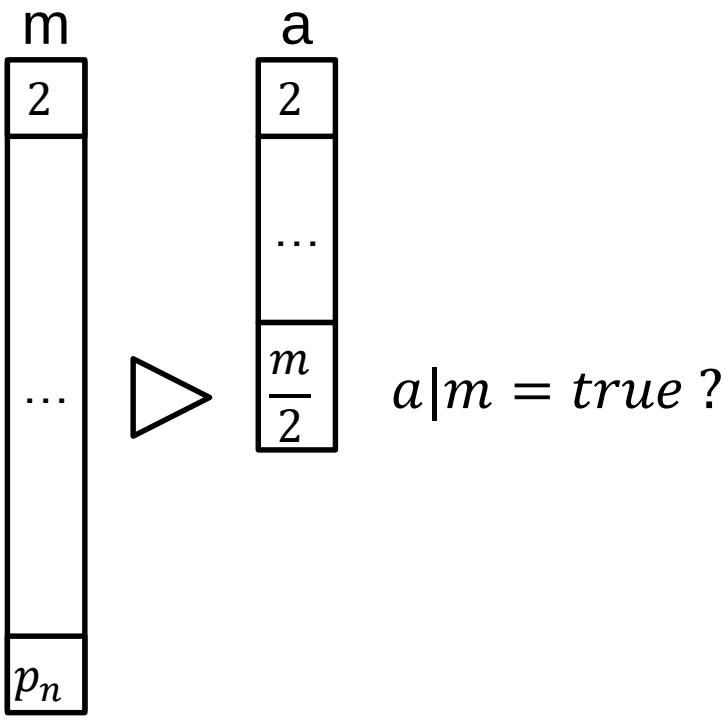
Implementierung

Schleifendurchläufe: Wormell‘sche Formel



Implementierung

Schleifendurchläufe: optimierte Methode

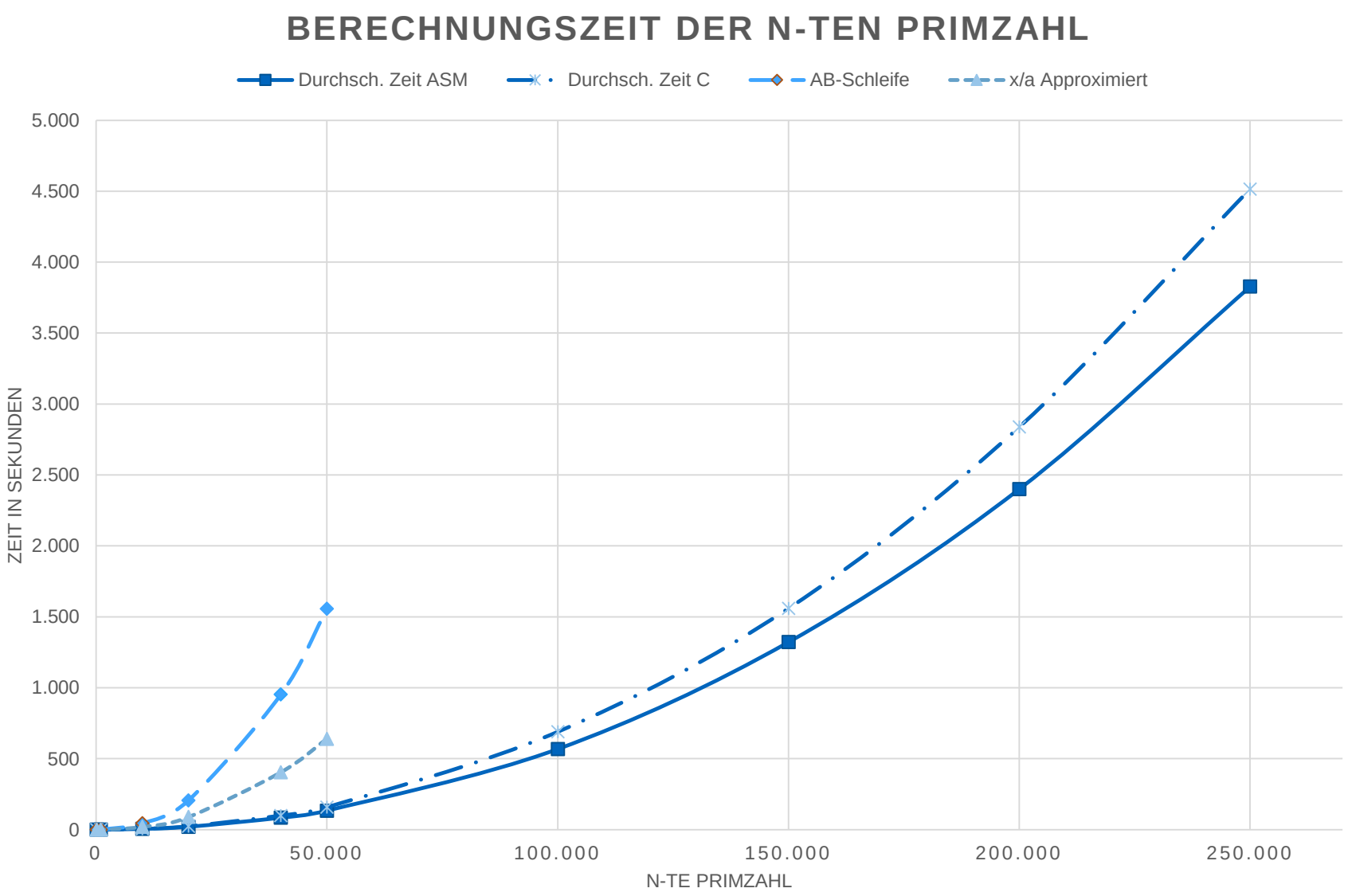


Implementierung

vdiv.F32 fpuReg, x, a	= x / a
vcvt.U32.F32 fpuReg, fpuReg	(int) Ergebnis
vmov armRegister, tmpReg	
mul armRegister, r3	a* Ergebnis
cmp armRegister, r1	== x ?
addeq r6, #1	AnzahlTeiler++
cmp r3, r1	Teiler == a?
subeq r6, #1	AnzahlTeiler--

Tabelle Berechnungsdauer

n-te Primzahl	k	Zeit ASM (Avg.)	Zeit C (Avg.)	C/ASM
100	100	0,0005270s	0,000625s	1,185
1000	100	0,03432s	0,04159s	1,211
10000	100	4,520s	5,46s	1,208
20000	10	19,43s	23,15s	1,190
40000	10	83,41s	98,60s	1,182
50000	10	133,26s	157,30s	1,180
100000	10	567,23s	688,63s	1,214
1	5	1320,93s	1558,60s	1,179
$2 * 10^6$	1	2400,19s	2837,87s	1,182
$2,5 * 10^6$	1	3827,20s	4514,93s	1,179


BERECHNUNGSZEIT DER N-TEN PRIMZAHL
Durchsch. Zeit ASM
Durchsch. Zeit C
AB-Schleife
x/a Approximiert
ZEIT IN SEKUNDEN
5.000
4.500
4.000
3.500
3.000
2.500
2.000
1.500
1.000
500
0
0
50.000
100.000
150.000
200.000
250.000
N-TE PRIMZAHL