Probleme 1

Primzahltests grundsätzlich Haftendorn Jan 2013

Primzahlsatz $\mathbf{pzs}(x) := \frac{x}{\ln(x)}$ ▸ *Fertig* *Approximiert die Anzahl der Primzahlen kleiner x*

siehe Graph−Fenster. Die Kurve wird für große x immer flacher

$\text{factor}\left(\frac{d}{dx}(\mathbf{pzs}(x))\right)$ ▸ $\frac{\ln(x)-1}{(\ln(x))^2}$ ⚠ $\lim_{x\to\infty}\left(\frac{\ln(x)-1}{(\ln(x))^2}\right)$ ▸ 0

In der Größenordnung der kryptografisch wichtigen Zahlen:

$\text{approx}\left(\frac{\ln(x)-1}{(\ln(x))^2}\,|\,x=2^{512}\right)$ ▸ 0.00281 ist die Steigung 0,28 %. Das heißt knapp 3 Tausendstel der Zahlen in einem Intervall in der Nähe von 2^512 sind Primzahlen.

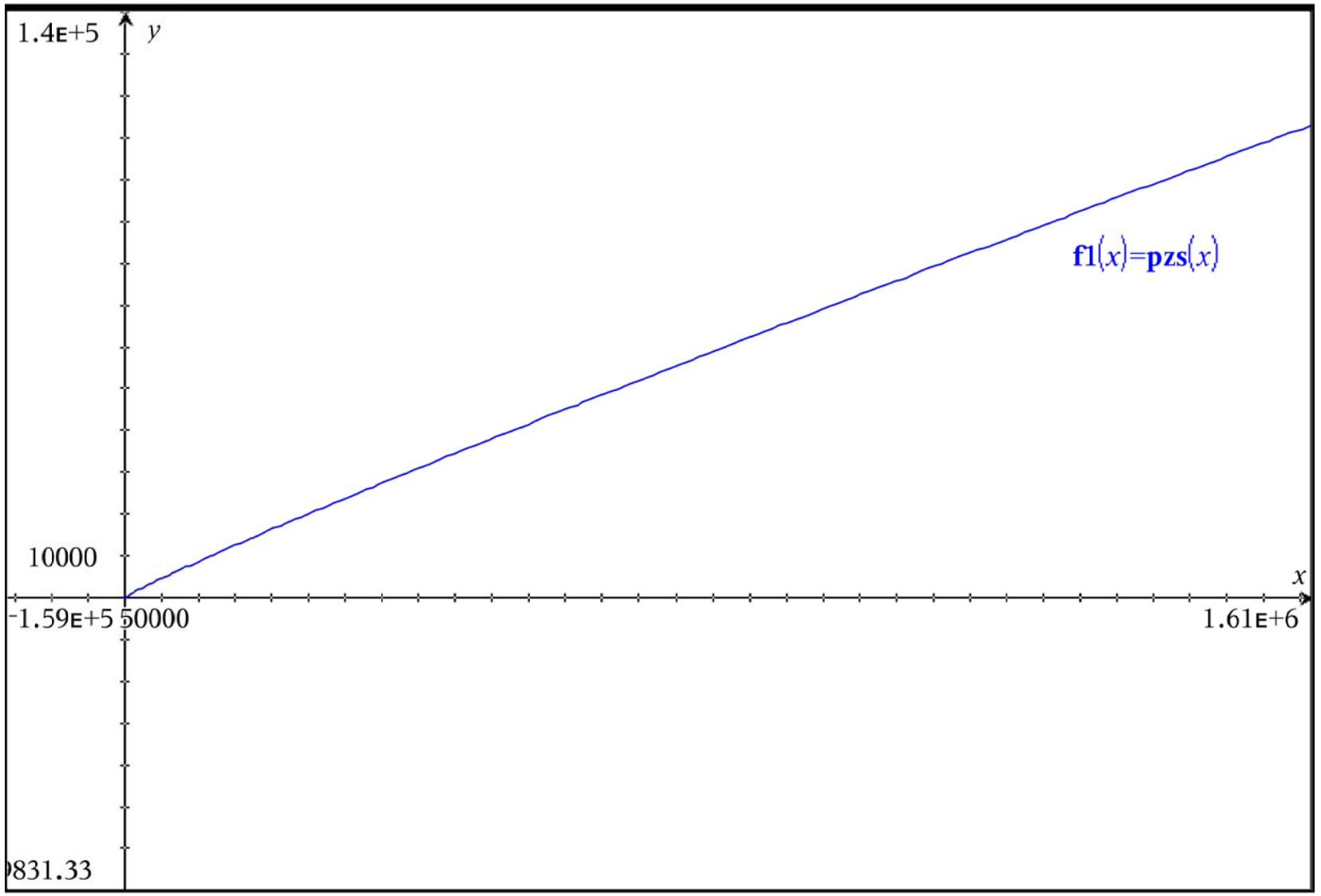
$\text{approx}(\mathbf{pzs}(2^{512}))$ ▸ 3.778E151 $\text{approx}(\mathbf{pzs}(2^{511}))$ ▸ 1.8927E151

$\mathbf{anz}(a,b) := \mathbf{pzs}(b) - \mathbf{pzs}(a)$ ▸ *Fertig* $\text{approx}(\mathbf{anz}(2^{511}, 2^{512}))$ ▸ 1.88531E151

Genauer: Zwischen 2^{511} ▸ 6.7039E153 und 2^{512} ▸ 1.34078E154

sind etwa $2\cdot 10^{151}$ Primzahlen.

1.1



1.2

$\mathbf{m}:=\frac{\text{approx}\left(\mathbf{anz}\left(2^{511},2^{512}\right)\right)}{2^{511}} \blacktriangleright 0.002812$ ist die Wahrscheinlichkeit, eine Primzahl durch zufälliges Herausgreifen zu erhalten. Die Zahl passt zur Steigung

$\frac{1}{\mathbf{m}} \blacktriangleright 355.587$ **im Mittel hat man nach 356 zufälligen Versuchen eine Primzahl gefunden.**

Das ein überschaubarer Aufwand.

Man testet dann z.B. mit dem Miller-Rabin-Test, ob man eine Primzahl gegriffen hat.

Zu dem Test gibt es die Funktion **istprim\istprim**$(n,wmax)$ oder eingebaut $\text{isprime}(n)$

Dabei ist wmax die Anzahl der Basen, die man probiert.

1.3

istprim\istprim(67567575757001,4) ▸ false Meine eigene Funktion verträgt keine längeren Argumente. isPrime(67567575757001) ▸ false

kry\nextprime(67567575757001) ▸ 67567575757013

istprim\istprim(67567575757013,4) ▸ true isPrime(67567575757013) ▸ true

isPrime(675675757570016756757777777777777777775555555555555555558888757013) ▸ false

kry\nextprime(675675757570016756757777777777777777775555555555555555558888757013)
▸ 675675757570016756757777777777777777775555555555555555558888757401

mod(675675757999999957013,67999999675757013) ▸ 24757612100000012726

Der Befehl, der die Begrenzung erzeugt, ist randInt(2,67675676575573) ▸ 53749212399204

Schade.

1.4