<u>Aufgabe</u>: Es wurde bereits ausgerechnet, dass die W'keit für eine Kollision $\frac{1}{2}$ beträgt, sofern der Zusammenhang zwischen n (der Anzahl der Zufallswerte) und m (die Größe des Zahlenintervalls für die Zufallszahlen)

$$n = 0{,}5 + 1{,}1774 \cdot \sqrt{m}$$ beträgt.

(Beispiel: Für $m = 365$ ergibt sich $n = 23$.)

Man berechne den Zusammenhang zwischen n und m für das 1. und das 3. Quartil (also für die W'keit $\frac{1}{4}$ und $\frac{3}{4}$)!

<u>Antwort</u>: Es wurde bereits abgeschätzt:

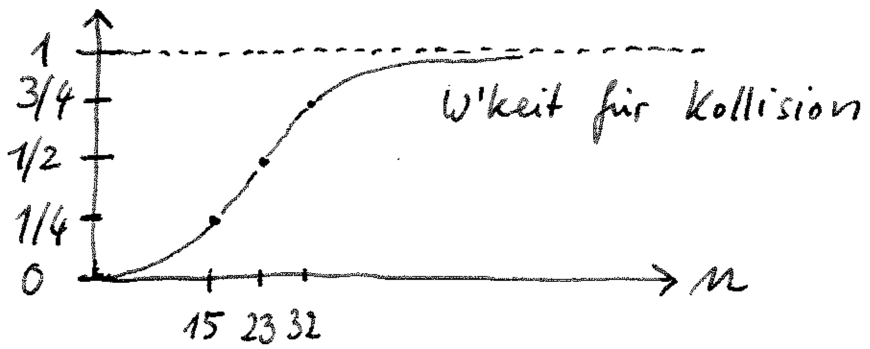
$$P(\text{alle } n \text{ Zufallswerte verschieden}) \approx e^{-(n-0{,}5)^2/2m}$$

Wir setzen die W'keit auf $\frac{3}{4}$ bzw $\frac{1}{4}$ und erhalten:

$$n = 0{,}5 + 0{,}759 \cdot \sqrt{m} \quad \text{(1. Quartil)}$$
$$n = 0{,}5 + 1{,}665 \cdot \sqrt{m} \quad \text{(3. Quartil)}$$

<u>Beispiel</u>: Bei $m = 365$ ergibt sich $n \approx 15$ (1. Quartil) und $n \approx 32{,}3$ (3. Quartil).

<u>Skizze</u>:



<u>Aufgabe</u>: Beim „Geburtstagsangriff" auf eine Hashfunktion hat man folgendes Szenario:

$x_1, x_2, \ldots, x_n$ --- Hashwerte der gutartigen Dokumente

$x_1', x_2', \ldots, x_n'$ --- Hashwerte der bösartigen Dokumente.

Wir nehmen an, die Hashfunktion erzeugt Zufallswerte im Intervall $\{1, 2, \ldots, m\}$. Man berechne die zu erwartende Anzahl Kollisionen (also solche (i,j) mit $x_i = x_j'$). Setze diesen Erwartungswert auf 1 und bestimme daraus einen Zusammenhang zwischen n und m!

<u>Antwort</u>: Es gibt n^2 viele Paare (i,j).
Bei jedem Paar kann mit W'keit $\frac{1}{m}$ eine Kollision auftreten. Die zu erwartende

Anzahl Kollisionen beträgt daher $n^2 \cdot \frac{1}{m}$.

Wir setzen $n^2 \cdot \frac{1}{m} \overset{!}{=} 1$ und erhalten

$\underline{n = \sqrt{m}}$.

Aufgabe: An der Kryptologie-Klausur schreiben 100 Studenten mit. Die Klausurergebnisse werden anschließend im Internet veröffentlicht. Aus „Sicherheitsgründen" gibt man dabei für jeden Studenten nur die letzten 3 Ziffern seiner Matrikelnummer an. Wie groß ist die Wahrscheinlichkeit, dass eine „Kollision" auftritt?

Antwort: Wir haben hier $n = 100$ und $m = 1000$. Die W'keit, dass keine Kollision auftritt, wurde abgeschätzt mit $e^{-(n-0{,}5)^2/2m} \underset{\substack{n=100\\m=1000}}{=} 0{,}007$.

Daher wird mit W'keit $0{,}993$ mindestens eine Kollision auftreten.

Aufgabe: [Geburtstagsangriff gegen den Diskreten Logarithmus]

Gegeben: n Primzahl und Primitivwurzel a modulo n. Sei $y \in \mathbb{Z}_n^*$ gegeben. Die algorithmische Aufgabe besteht darin, ein x zu finden, so dass $y \equiv a^x \pmod{n}$.

Algorithmus: Fülle die Menge $\mathcal{M}$ nach und nach mit Zufallszahlen $z_1, z_2, \ldots < n$, bis man i, j findet $(i \neq j)$ mit $y \cdot a^{z_i} \equiv a^{z_j} \pmod{n}$

Wenn ein solches Paar gefunden ist, gilt:

$$y \equiv a^{z_j - z_i} \pmod{n}.$$

Liefere also $z_j - z_i$ als Ergebnis ab (bzw. $(z_j - z_i) \bmod (n-1)$). Wie groß wird $\mathcal{M}$ durchschnittlich, bis man auf diese Weise den diskreten Logarithmus bestimmt hat?

Antwort: Wegen Geburtstagsparadoxon:

$$E\left(|\mathcal{M}|\right) = O(\sqrt{n}).$$

Blinde Unterschrift

A erstellt ein Dokument m und möchte, dass dieses von B unterschrieben wird; A möchte also $\underbrace{D(k_B', m)}$ erhalten.

bei RSA: $m^d \bmod n$, wobei (d,n) geheimer Schlüssel von B.

Das Dokument m soll von B aber nicht gelesen werden können; m soll also irgendwie geeignet verschlüsselt sein.

$$\begin{tikzcd}
A: \quad m \arrow[rr, "\text{B kann m}", "\text{lesen}"'] \arrow[d, "\text{A das}"', "\text{„verblendet“ Dokument m}"] & & m, \text{ mit B's Unterschrift} \\
\hat{m} \arrow[rr, "\text{B kann m}", "\text{nicht lesen}"'] & & \hat{m}, \text{ mit B's Unterschrift} \arrow[u, "\text{A entfernt die Verblendung}"']
\end{tikzcd}$$

Im Kontext von RSA lässt sich dies umsetzen:

A	B
hat Dokument m.	
besorgt sich den öffentlichen RSA-Schlüssel (e, n) von B.	
Wählt Zufallszahl $z \in \mathbb{Z}_n^*$	
berechnet $\hat{m} = m \cdot z^e \bmod n$	
$\xrightarrow{\hat{m}}$	
	unterschreibt $\hat{m}$, berechnet also $m' = (\hat{m})^d \bmod n$ (d = geheimer Schlüssel von B)
$\xleftarrow{m'}$	
berechnet mittels ExtEuklid die Zahl $z^{-1} \bmod n$.	
Berechnet $m'' = m' \cdot z^{-1} \bmod n$	

Nun ist m'' das von B unterschriebene Dokument m.

Begründung:

$$m'' = m' \cdot z^{-1} = (\hat{m})^d \cdot z^{-1}$$
$$= (m \cdot z^e)^d \cdot z^{-1} = m^d \cdot z \cdot z^{-1} = m^d$$

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

$$e \cdot d = 1 + k \cdot \varphi(n)$$

$$z^{e \cdot d} = z^{1 + k \cdot \varphi(n)} = z \cdot \left(z^{\varphi(n)}\right)^k$$
$$= z \cdot 1^k = z$$

Legendre-Symbol:

Sei p Primzahl; $x \in \mathbb{Z}_p^*$:

$$\left(\frac{x}{p}\right) := \begin{cases} 1, & \text{falls } x \in QR_p \\ -1, & \text{falls } x \in QNR_p \end{cases}$$

Wir wissen bereits (Euler-Kriterium):

$$x^{\frac{p-1}{2}} \equiv \left(\frac{x}{p}\right) \pmod p$$

Somit kann man das Legendre-Symbol durch eine modulare Exponentiation $\mathrm{modexp}(x, (p-1)/2, p)$ mit Rechenzeit $O(m^3)$ berechnen (m ... Bitlänge).

Bem: Sofern $x \in QR_p$, so kann man ebenfalls durch eine modulare Exponentiation eine Quadratwurzel von x berechnen (sofern $p \equiv 3 \pmod 4$), nämlich:

$$\text{„}\sqrt{x}\text{"} = \mathrm{modexp}(x, (p+1)/4, p).$$

Rechenaufwand: $O(m^3)$.

Auch im anderen Fall ($p \equiv 1 \pmod 4$) lässt sich die Quadratwurzel von x effizient berechnen (Aufwand $O(m^4)$). Man benötigt einen quadratischen Nichtrest $b \in QNR_p$. Solches b erfüllt das „Anti-Euler-Kriterium“: $b^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Der Vollständigkeit halber hier nochmals der Algorithmus zur Berechnung der Quadratwurzel von x in diesem Fall ($p \equiv 1 \pmod 4$):

$e := (p-1)/2$;
$f := 0$;
<u>repeat</u>
    $e := e/2$;
    $f := f/2$;
    <u>if</u> $x^e \cdot b^f \equiv -1 \pmod p$ <u>then</u>
        $f := (f + (p-1)/2) \bmod (n-1)$;
<u>until</u> e ungerade;
<u>return</u> $x^{(e+1)/2} \cdot b^{f/2} \bmod n$.

Das Jacobi-Symbol verallgemeinert das Legendre-Symbol dahingehend, dass nun n keine Primzahl sein muss. Sei $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ die Primfaktorisierung von n.

Nun definiert man für $x \in \mathbb{Z}_n^*$:

$$\underbrace{\left(\frac{x}{n}\right)}_{\text{Jacobi-Symbol}} := \left(\frac{x}{p_1}\right)^{e_1} \cdot \left(\frac{x}{p_2}\right)^{e_2} \cdots \left(\frac{x}{p_k}\right)^{e_k}$$

jeweils Legendre-Symbole.

Da die Legendre-Symbole auf der rechten Seite nur $+1$ oder -1 sein können, ergeben alle Ausdrücke $\left(\frac{x}{p_i}\right)^{e_i}$ mit geradzahligem e_i den Wert 1.

Beispiel: Sei $n = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7^1 \cdot 11^2$, dann ist

$$\left(\frac{x}{n}\right) = \left(\frac{x}{3}\right) \cdot \left(\frac{x}{7}\right),$$

da nur bei 3 und bei 7 ungeradzahlige Exponenten auftreten.

Trotzdem, das Berechnen des Jacobi-Symbols scheint schwieriger zu sein als das Berechnen des Legendre-Symbols, da man die Faktorisierung von n benötigt (zumindest wenn man der Definition des Jacobi-Symbols folgt).

Wir zitieren einige Eigenschaften des Jacobi-Symbols:

- Multiplikativität: $\left(\frac{xy}{n}\right) = \left(\frac{x}{n}\right) \cdot \left(\frac{y}{n}\right)$

  $$\left(\frac{x}{m \cdot n}\right) = \left(\frac{x}{m}\right) \cdot \left(\frac{x}{n}\right)$$

- Falls $a \equiv b \pmod{n}$, dann ist $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

  Insbesondere (wenn $a > n$), so kann man rechnen: $\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right)$.

- Der Sonderfall $a = 2$:

  $$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} 1, & \text{falls } n \equiv \pm 1 \pmod{8} \\ -1, & \text{falls } n \equiv \pm 3 \pmod{8} \end{cases}$$

– Quadratisches Reziprozitätsgesetz (Gauß):

Seien $m, n \geq 3$ ungerade Zahlen.

$$\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4} \cdot \left(\frac{n}{m}\right)$$

wobei $(-1)^{(n-1)(m-1)/4} = \begin{cases} -1, & \text{falls } n \equiv m \equiv 3 \pmod 4 \\ 1, & \text{sonst.} \end{cases}$

Eine <u>Beispielrechnung</u>:

$$\left(\frac{35}{1683}\right) \underset{(QR)}{=} -\left(\frac{1683}{35}\right) = -\left(\frac{1683 \bmod 35}{35}\right) = -\left(\frac{3}{35}\right)$$

$$\underset{(QR)}{=} \left(\frac{35}{3}\right) = \left(\frac{35 \bmod 3}{3}\right) = \left(\frac{2}{3}\right) \underset{\text{(Sonderfall)}}{=} -1$$

<u>proc</u> Jacobi (m, n) ... berechnet $\left(\frac{m}{n}\right)$

$m := m \bmod n$;

<u>if</u> $m = 1$ <u>then</u> <u>return</u> 1;

// Sei jetzt $m = 2^t \cdot u$ wobei u ungerade

Berechne $w = \left(\frac{2^t}{n}\right) = \left(\frac{2}{n}\right)^t$ mit Sonderfall-Regel

<u>if</u> $u = 1$ <u>then</u> return w;

<u>return</u> $w * (-1)^{(n-1)(u-1)/4} *$ Jacobi(n, u);

Wie bei Euklid: Laufzeit $\mathcal{O}(m^2)$

Eine mögliche Anwendung: der Solovay-Strassen-Primzahltest:

Eingabe n

Wähle $a < n$ zufällig

Jacobi(a, n)

if $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ <u>then</u>

„wahrscheinlich Primzahl"

mod. Exp:
modexp(a, (n-1)/2, n)

<u>else</u> „keine Primzahl"

$$
\begin{tikzcd}
n \text{ Primzahl} \arrow[r] & \text{„wahrsch. Primzahl"} \\
n \text{ keine Primzahl} \arrow[ur, "\frac{1}{2}"] \arrow[r, "\frac{1}{2}"'] & \text{„keine Primzahl"}
\end{tikzcd}
$$