

Übungen zur Vorlesung Kryptographie

## Blatt 4

**Aufgabe 13: (Genug Primzahlen?)**

Die Aufgabe ist, zu bestimmen, wieviele 16-bit-Primzahlen es gibt, und wieviele 24-bit-Primzahlen. Genauer:

- (a) Bestimmen Sie mit dem Primzahlsatz (Satz 3.1 im Skript), wieviele Primzahlen es zwischen  $2^{k-1}$  und  $2^k$  geben sollte, jeweils für  $k = 16$  und  $k = 24$ .
- (b) Zählen Sie (mit dem Rechner) wieviele Primzahlen es zwischen  $2^{k-1}$  und  $2^k$  wirklich gibt, jeweils für  $k = 16$  und  $k = 24$ .

**Aufgabe 14: (Alles Lügner / Primzahl entlarven)**

- (a) Finden Sie drei Zahlen  $n \in \mathbb{N} \setminus \{1\}$ , die keine Primzahlen sind, so dass dennoch für alle  $a \in \mathbb{N}$  mit  $2 \leq a \leq n - 1$  gilt: Falls  $\text{ggT}(a, n) = 1$ , so ist  $a^{n-1} \equiv 1 \pmod n$ .
- (b) Eine der Zahlen  $10^{200} + 349$  und  $10^{200} + 357$  ist eine Primzahl, die andere nicht. Finden Sie mit dem Fermattest heraus, welche was ist.

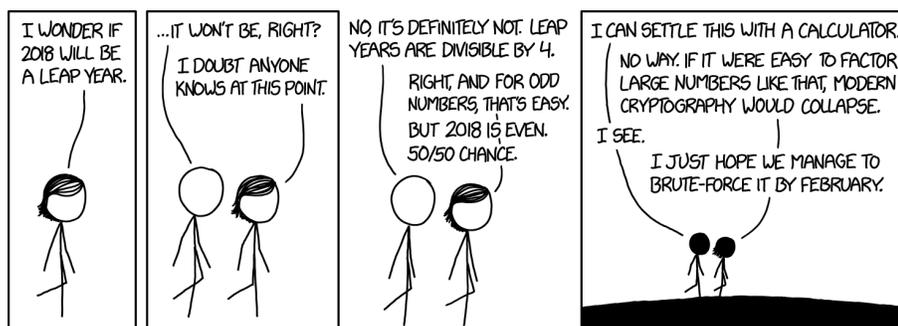
*(Nutzen Sie den Fermattest, nicht etwa `is_prime` oder `next_prime` oder Ähnliches. Obacht, nicht alle Befehle sind gleich gut geeignet, um die benötigten Terme zu berechnen!)*

**Aufgabe 15: (Wieviele Fermat-Lügner?)**

- (a) Finden Sie alle Fermat-Lügner mod 21 und alle Fermat-Lügner mod 91.
- (b) Zeigen Sie: sind  $p$  und  $2p - 1$  beides Primzahlen, sowie  $n = p(2p - 1)$ , so sind alle  $a \in Z_n^*$ , die quadratische Reste mod  $2p - 1$  sind, Fermat-Lügner mod  $n$ .

**Aufgabe 16: (Wieviele Miller-Rabin-Lügner?)**

Finden Sie alle Miller-Rabin-Lügner für  $N = 145$ . Das heißt, finden Sie  $a \in \{2, 3, \dots, 143\}$ , so dass der Miller-Rabin-Test für dieses  $a$  ausgibt "145 ist wahrscheinlich Primzahl".



xkcd.com

Abgabe bis Mittwoch 6.5.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann    pbraukmann@techfak.de  
Jonas Friemel        jfriemel+krypto@techfak.de