1.5. St. Moritz, Gloria Klub (3605 m ü. NN)

Bond: Gut, dass ich Sie spreche, Q! Ich habe seit kurzem Probleme mit der Schlüsselerzeugung in meinem Wagen. Muss an der Kälte liegen. Die automatische Primzahlerzeugung funktioniert nicht mehr korrekt.

Q: Das Problem ist bekannt. Bei großer Kälte versagt der dafür zuständige Chip im BMW relativ häufig. Erzeugen Sie doch Ihre Primzahlen solange von Hand. Sie erinnern sich an den Primtest von Fermat?

Bond: Fermat war doch dieser Hobbymathematiker aus dem 17. Jahrhundert, der diese berühmte Vermutung aufgestellt hat, richtig?

Q: Korrekt. Außerdem entwickelte er den ersten schnellen Primtest...

Bond: ...der darauf beruht, dass für eine Primzahl p und alle Zahlen a, $0 < a < p$, gilt, dass p die Zahl $a^{p-1} - 1$ teilt.

Überprüft, dass diese Aussage tatsächlich stimmt: Sucht Euch ein kleines n (sagen wir, kleiner 500) aus, rechnet $\frac{a^{n-1}-1}{n}$ für alle $0 < a < n$ aus und prüft, wann das eine ganze Zahl ist. Könnt Ihr anhand der Ausgabe erkennen, ob Eure Zahl n prim ist?

Q: Sie merken sich auch alles! Wichtig ist, dass Sie Ihren Primzahlgenerator schnell reparieren, damit wir wieder mittels RSA kommunizieren können.

Bond: Geht klar, mache mich sofort an die Arbeit.

Helft Bond die Aufgabe zu lösen: Schreibt Euren eigenen Primzahlgenerator, der die Fermat-Gleichung von oben benutzt:

```
myisprime:=proc(p) begin
  ...; res:=powermod( a, ..., p ); return( res=1 );
end_proc:
```

Fragen

- *Wie lange würde es dauern, alle möglichen Teiler einer 100-stelligen Zahl durchzuprobieren, wenn eine Division 1µs benötigt?*
- *Eigentlich genügt es viel weniger zu tun: Wenn die Zahl nicht prim ist, dann muss ein Teiler kleiner als die Wurzel sein. Wie lange würde das nun brauchen?*
- *Der Test mit der Fermat-Gleichung ist noch viel schneller, allerdings nicht hundertprozentig. Man braucht ihn (in der richtigen Form) nur 20 mal zu wiederholen, um mit einer Wahrscheinlichkeit von 1 zu 1 048 576 die richtige Antwort zu finden. Fragt danach...*