Sieb des Eratosthenes

Suchen alle Primzahlen bis zu einer Zahl $n \in \mathbb{N}$. Dazu: $n := 36$ $\sqrt{n} = 6$

2 3 4 5 6 7 8 9 10 11
12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
32 33 34 35 36

Hier sei entsteht eine weitere Idee:

$$P := \prod_{i \in I} p_i \qquad p_i \text{ Primzahlen}$$

$ggT(P, N) \neq 1$, so haben wir Teiler unter den p_i

$= 1$, so wissen wir, dass keines der p_i N teilt

Man sollte sich eine Strategie ausdenken für beliebige N.

Fermats Idee

Sei $N \in \mathbb{N}$ ungerade und eine zusammengesetzte Zahl, also

$N = a \cdot b$ $\quad a, b \in \mathbb{N}$ ungerade

Durch die Wahl von $x, y \in \mathbb{N}$ mit

$$x := \frac{a+b}{2} \quad \text{und} \quad y := \frac{a-b}{2}$$

können wir auch schreiben:

$$N = (x+y)(x-y) = x^2 - y^2$$

Wir suchen also ein Quadrat, das die folgende Gleichung erfüllt:

$$y^2 = x^2 - N$$

Dazu beschreib Fermat folgenden Algorithmus:

(1) $x := \lfloor \sqrt{N} \rfloor + 1$ $\qquad f(x) = x^2 - N$

(2) Ist nun $f(x) = y^2$ ein Quadrat, so haben wir die Faktorisierung $N = a \cdot b = (x+y)(x-y)$

Wenn nicht:

$x := x + 1$ $\quad$ und $\quad f(x+1) = (x+1)^2 - N$

$= f(x) + 2x + 1$

und starte (2) neu.