

# Sieb des Eratosthenes

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

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

Hier bei entsteht eine weitere Idee:

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

$\text{ggT}(p, N) \neq 1$ , 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

$$N = a \cdot b$$

$a, b \in \mathbb{N}$  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 beschrieb Fermat folgenden Algorithmus:

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

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

Wenn nicht:

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

und starte (2) neu.

# Erweiterung der Idee

(durch Gauß (1777-1855), Legendre (1752-1833) und später in den 20er Jahren Kratichik (1887-1957))

Sie fanden heraus, das man auch folgendes suchen kann:

$$x^2 - y^2 = (x+y)(x-y) = kN \quad k \in \mathbb{N}$$

Daraus folgt, dass in dem Restklassenring  $\mathbb{Z}/N\mathbb{Z}$  für  $x^2$  die Wurzel  $y$  ex.

Wir suchen also:

$$x^2 \equiv_N y^2 \quad \text{mit} \quad x \not\equiv_N \pm y$$

Finden wir ein solches  $y$ , so können wir über den

$$\text{ggT}(x-y, N)$$

einen nicht-trivialen Teiler von  $N$  finden.

Allg. Vorgehensweis bei den im Folgenden beschriebenen Algorithmen:

Wir bestimmen quadratische Reste

$$z_i \equiv_N x_i^2 \quad z_i \in \mathbb{Z} \quad i \in S := \{1, \dots, s\}$$

und versuchen durch geschickte Wahl von  $I \subseteq S$  folgendes zu finden:

$$\prod_{i \in I} z_i = y^2 \quad \text{ein Quadrat in } \mathbb{Z};$$

$$\text{wähle dann:} \quad x := \prod_{i \in I} x_i$$

$$\Rightarrow x^2 \equiv_N y^2$$

$$y^2 \equiv_N x^2 \quad \text{mit} \quad x \not\equiv_N \pm y$$

Es gibt genau  $2^d$  verschiedene  
Wurzeln von  $x^2$  ( $d \equiv$  Anzahl Primfaktoren von  $N$ )

Zur Ex. von solchen  $y$ :

Sei dazu  $N$  ungerade, keine Primzahl

Sei  $N = a \cdot b$   $a, b$  teilerfremd

$$y \in \mathbb{Z}_N^*$$

$$\stackrel{\text{CRS}}{\Rightarrow} \exists x \in \mathbb{Z}_N^* \quad \text{mit} \quad \underbrace{x \equiv_a y}_{*} \quad x \equiv_b -y$$

$$\text{d.h.} \quad a \mid x - y \quad \text{und} \quad b \mid x + y$$

$$\text{also:} \quad x^2 \equiv_N y^2$$

Es bleibt zu zeigen,  $x \not\equiv \pm y$

Nehmen das Gegenteil an  $x \equiv_N +y$  oder  $x \equiv_N -y$

$$\subseteq x \equiv_N -y$$

$$\Rightarrow x \equiv_a -y \quad \text{aber auch} \quad x \equiv_a y \quad (*)$$

$$\Rightarrow 2x \equiv_a 0 \quad \text{da } a \text{ ungerade} \Rightarrow a \mid x$$

$$\Rightarrow \text{ggT}(x, N) \neq 1 \quad \text{⚡} \quad x \in \mathbb{Z}_N^*$$

Dazu müssen wir uns Folgendes vorstellen:

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_d^{e_d}\mathbb{Z}$$

$$z = (z_1, \dots, z_d)$$

$$(y_1^2, \dots, y_d^2) = y^2$$

Wurzeln von  $(z_1, \dots, z_n)$

sind demnach  $(\pm y_1, \dots, \pm y_d)$

Warum gibt es (genau)  $2^d$  Stück, obwohl wir uns in Ringen befinden?

Dazu:

Es existieren keine oder zwei Quadratwurzeln einer Zahl  $a \in \mathbb{Z}/p^e\mathbb{Z}$   $a \neq 0, p \neq 2$

Seien  $x, y \in \mathbb{Z}/p^e\mathbb{Z}$  Quadratwurzeln von  $a$

Dann ist  $x^2 - y^2 = kp^e$   $k \in \mathbb{Z}$

also  $(x+y)(x-y) = kp^e$  (\*)

Es kann aber nicht sein, dass  $x+y$  und  $x-y$  durch  $p^e$  teilbar sind, dann würde folgen

$$y \equiv_{p^e} -y \Rightarrow y=0 \Rightarrow a = y^2 = 0 \nrightarrow (*)$$

Also ist entweder  $x+y$  oder  $x-y$  teilbar durch  $p^e$  (nach \*)

$$\Rightarrow x=y \text{ oder } x=-y$$

