Contents

1 Dixon

- Smoothiefunktion $f_n(x) = x^2 \pmod n$, Faktorbasis P festlegen
- Große Menge S an Smoothies finden
- Teilmenge $S_d \subseteq S$ finden, so dass $y^2 := \prod_{s \in S_d} f(s)$ ein Quadrat ist
- $y^2 := \prod_{s \in S_d} f(s) \equiv \prod_{s \in S_d} s^2 = \left(\underbrace{\prod_{s \in S_d} s}_{=:x} \right)^2 = x^2 \pmod n$
- Smoothies finden durch: Irgendwelche Zahlen s testen, ob $f(s)$ smooth ist

2 Quadratisches Sieb

- $f_n(x) = x^2 - n$
- Alles funktioniert wie vorher
- Smoothies suchen im Array
- $p | f(x) \Rightarrow p | f(x-p)$, denn:

$$f(x-p) = (x+p)^2 - n = x^2 - 2xp + p^2 - n = f_n(x) + 2xp + p^2$$

- Mit jedem p aus der Faktorbasis durchsieben, man braucht nur die Startwerte
- Startwerte durch $f_n(x) \equiv 0 \pmod p$

$$
\begin{aligned}
x^2 =& \phi\left(\beta\right)^2 \\
=& \phi(\beta^2) \\
=& \phi\left(\prod_{s \in S_d} f_M\left(s\right)\right) \\
=& \prod_{s \in S_d} \phi\left(f_M\left(s\right)\right) \\
\equiv& \prod_{s \in S_d} f_{\mathbb{Z}_n}\left(s\right) \\
=& y^2
\end{aligned}
$$

- Frage: Wie findet man Quadrate in M? Wir werden zwei Möglichkeiten gleichzeitig benutzten.
- S und M können aus irgendwelchen Grundmengen sein
- $S = \mathbb{Z}^2$, $M = \mathbb{Z}[\theta]$ für einen Zahlkörper $\mathbb{Q}(\theta)$