Challenge!

Seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Gebe einen $\mathcal{O}(n)$ Algorithmus an, der eine zusammenhängende Teilfolge $a_i, a_{i+1}, \ldots, a_j$ findet mit $1 \leq i \leq j \leq n$, so dass $n \mid (a_i + a_{i+1} + \ldots + a_j)$.
Eine genaue Laufzeitanalyse vom angegebenem Algorithmus ist nicht nötig.

Tipp: Betrachte die Summen $S_i := \sum_{k=1}^{i} a_k$ für $1 \leq i \leq n$.

Die Eulerfunktion

Recap

Die Eulerfunktion φ gibt uns die Anzahl Elemente in $\mathbb{Z}_n$, die teilerfremd sind zu n.

Die Eulerfunktion

Recap

Die Eulerfunktion φ gibt uns die Anzahl Elemente in $\mathbb{Z}_n$, die teilerfremd sind zu n.

Lemma

Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung einer Zahl n. Dann ist

$$|\mathbb{Z}_n^*| = \varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}.$$

In anderen Worten gibt uns $\varphi(n)$ die Ordnung der multiplikativen Gruppe $\mathbb{Z}_n^*$.

Die Eulerfunktion

Recap

Die Eulerfunktion φ gibt uns die Anzahl Elemente in $\mathbb{Z}_n$, die teilerfremd sind zu n.

Lemma

Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung einer Zahl n. Dann ist

$$|\mathbb{Z}_n^*| = \varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}.$$

In anderen Worten gibt uns $\varphi(n)$ die Ordnung der multiplikativen Gruppe $\mathbb{Z}_n^*$.

Beispiel

Sei $n = 18 = 2 \cdot 3^2$. Dann ist $\varphi(n) =$

Die Eulerfunktion φ gibt uns die Anzahl Elemente in $\mathbb{Z}_n$, die teilerfremd sind zu n.

Lemma

Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung einer Zahl n. Dann ist

$$|\mathbb{Z}_n^*| = \varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}.$$

In anderen Worten gibt uns $\varphi(n)$ die Ordnung der multiplikativen Gruppe $\mathbb{Z}_n^*$.

Beispiel

Sei $n = 18 = 2 \cdot 3^2$. Dann ist $\varphi(n) = (2-1)2^0 \cdot (3-1)3^1 = 6$.

Wir erinnern uns an folgendes wichtige Lemma:

Wir erinnern uns an folgendes wichtige Lemma:

Lemma

Sei G eine endliche Gruppe mit Neutralelement e. Dann gilt für alle $a \in G$:

$$a^{|G|} = e$$

Die Eulerfunktion

Recap

Wir erinnern uns an folgendes wichtige Lemma:

Lemma

Sei G eine endliche Gruppe mit Neutralelement e. Dann gilt für alle $a \in G$:

$$a^{|G|} = e$$

Daraus folgt ganz einfach:

Lemma

Für alle $a \in \mathbb{Z}_n^*$:

$$a^{\varphi(n)} \equiv_n 1$$

Die Eulerfunktion

Recap

Wir erinnern uns an folgendes wichtige Lemma:

Lemma

Sei G eine endliche Gruppe mit Neutralelement e. Dann gilt für alle $a \in G$:

$$a^{|G|} = e$$

Daraus folgt ganz einfach:

Lemma

Für alle $a \in \mathbb{Z}_n^*$:

$$a^{\varphi(n)} \equiv_n 1$$

und für eine Primzahl p, für alle $1 \leq a < p$:

$$a^{p-1} \equiv_p 1$$

Aufgabe 1

Let $c = 7$ be a message encrypted with the public key pair (n, e). Find both the secret key d and the original message m.

Modulare Arithmetik Tricks

Innerhalb von $R_n(\ldots)$ dürfen wir alles machen, was wir wollen, solange wir die Kongruenz Modulo n der Terme nicht verändern, **ausser in den Exponenten.**

Modulare Arithmetik Tricks

Innerhalb von $R_n(\ldots)$ dürfen wir alles machen, was wir wollen, solange wir die Kongruenz Modulo n der Terme nicht verändern, **ausser in den Exponenten.**

- $R_3(5^3) = R_3(R_3(5)^3) = R_3(2^3) = R_3(8) = 2$

Modulare Arithmetik Tricks

Innerhalb von $R_n(\ldots)$ dürfen wir alles machen, was wir wollen, solange wir die Kongruenz Modulo n der Terme nicht verändern, **ausser in den Exponenten.**

- $R_3(5^3) = R_3(R_3(5)^3) = R_3(2^3) = R_3(8) = 2$
- $R_3(5^3) \neq R_3(5^{R_3(3)}) = R_3(5^0) = 1$

Modulare Arithmetik Tricks

Kongruenz zu 1

Berechne

$$R_{18}(37^{42}) =$$

Modulare Arithmetik Tricks

Kongruenz zu 1

Berechne

$$R_{18}(37^{42}) = 1$$

Modulare Arithmetik Tricks

Der "-" Trick

Berechne

$$R_3(5^{2022}) =$$

Modulare Arithmetik Tricks

Der “-” Trick

Berechne

$$R_3(5^{2022}) = 1$$

Modulare Arithmetik Tricks

Fermat's Little Theorem

Berechne

$$R_7(1984^6) =$$

Hint: 7 teilt 1984 nicht.

Modulare Arithmetik Tricks

Fermat's Little Theorem

Berechne

$$R_7(1984^6) = 1$$

Hint: 7 teilt 1984 nicht.

Modulare Arithmetik Tricks

Fermat's Little Theorem

Berechne

$$R_{11}(2^{1408}) =$$

Modulare Arithmetik Tricks

Fermat's Little Theorem

Berechne

$$R_{11}(2^{1408}) = 3$$

Modulare Arithmetik Tricks

Fermat's Little Theorem

Berechne

$$R_{11}(2^{3^{40}}) =$$

Modulare Arithmetik Tricks

Fermat's Little Theorem

Berechne

$$R_{11}(2^{3^{40}}) = 2$$

Kahoot!