UNENDLICHKEIT DER PRIMZAHLEN

Behauptung: Es gibt unendlich viele Primzahlen

1. Beweis von Euklid

2. Beweis mithilfe der Fermat-Zahlen

3. Beweis mithilfe der Eulerschen Phi-Funktion

4. Beweis mithilfe der Mersenne-Zahlen

1. Beweis von Euklid

- Def. **Primzahlen :**

  Natürliche Zahl **p** ist eine Primzahl, falls **p** nur durch **1** und **p** teilbar ist.

1. Beweis von Euklid

- Def. **Primzahlen :**

  Natürliche Zahl **p** ist eine Primzahl, falls **p** nur durch **1** und **p** teilbar ist.

- Def. **Primfaktorzerlegung :**

  Jede natürliche Zahl **n ≥ 2** ist entweder selbst eine Primzahl oder lässt sich als Produkt von (mindestens zwei) Primzahlen schreiben. Diese Primfaktoren sind eindeutig. Beispiel: 36 = 2 * **18** = 2 * 2 * **9** = 2 * 2 * 3 * 3

1. Beweis von Euklid

Annahme : Es gibt endlich viele Primzahlen $\{ p_1, \ldots, p_r \}$ *. . .*

1. Beweis von Euklid

Annahme : Es gibt endlich viele Primzahlen $\{ p_1, \ldots, p_r \}$ *. . .*

Beweis :

Sei **n := $p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$** und **p** ein Primteiler von **n**, also **p|n**

1. Beweis von Euklid

Annahme : Es gibt endlich viele Primzahlen $\{ p_1, \ldots, p_r \}$ . . .

Beweis :

Sei **n := $p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$** und **p** ein Primteiler von **n**, also **p|n**

⇒ **p** von allen p_i verschieden, da sonst **p|n** als auch **p|$p_1 \cdot p_2 \cdot \ldots \cdot p_r$** und somit auch **p|1** ↯

2. Beweis mithilfe der Fermat-Zahlen

- Def. **Fermat-Zahlen :** $F_n = 2^{2^n} + 1$,$n \geq 0$ $F_0 = 3,\quad F_1 = 5,\quad F_2 = 17,\ \ldots$

2. Beweis mithilfe der Fermat-Zahlen

- Def. **Fermat-Zahlen :** $F_n = 2^{2^n} + 1 \quad ,n \geq 0$ $\quad F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \ \ldots$

Beweisidee :

Zu zeigen : Je 2 Fermat-Zahlen sind relativ prim (teilerfremd).

Dazu beweisen wir die Rekursion : $\prod_{k=0}^{n-1} F_k = F_n - 2 \quad ,n \geq 1$

2. Beweis mithilfe der Fermat-Zahlen

- Def. **Fermat-Zahlen :** $F_n = 2^{2^n} + 1 \quad ,n \geq 0 \qquad F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \ \ldots$

Beweisidee :

Zu zeigen : Je 2 Fermat-Zahlen sind relativ prim (teilerfremd).

Dazu beweisen wir die Rekursion : $\prod_{k=0}^{n-1} F_k = F_n - 2 \qquad ,n \geq 1$

Beweis :

Sei **m** gemeinsamer Teiler von $\mathbf{F_K}$ und $\mathbf{F_n}$ $(k < n)$ $\Rightarrow$ **m** muss auch 2 teilen

$\Rightarrow m = 1$ oder $m \not= 2$ $\Rightarrow F_k$ und F_n paarweise teilerfremd $\Rightarrow$ Weil F_n unendlich $\Rightarrow$ P unendlich

2. Beweis mithilfe der Fermat-Zahlen

- Def. **Fermat-Zahlen :** $F_n = 2^{2^n} + 1$, $n \geq 0$ $F_0 = 3,\quad F_1 = 5,\quad F_2 = 17,\ \ldots$

  Z.z. : $\prod_{k=0}^{n-1} F_k = F_n - 2$, $n \geq 1$ (*)

  Beweis per Induktion :

  IA: für n=1 gilt: $F_0 = F_1 - 2 = 3$ $\Rightarrow$ IV: (*)

2. Beweis mithilfe der Fermat-Zahlen

- Def. **Fermat-Zahlen :** $F_n = 2^{2^n} + 1$, $n \geq 0$ $F_0 = 3,\quad F_1 = 5,\quad F_2 = 17,\ \ldots$

  Z.z. : $\prod_{k=0}^{n-1} F_k = F_n - 2$, $n \geq 1$ (*)

  Beweis per Induktion :

  IA: für n=1 gilt: $F_0 = F_1 - 2 = 3$ $\Rightarrow$ IV: (*)

  IB: n=n+1: $\prod_{k=0}^{n} F_k = F_{n+1} - 2$

2. Beweis mithilfe der Fermat-Zahlen

- Def. **Fermat-Zahlen :** $F_n = 2^{2^n} + 1$, $n \geq 0$ $F_0 = 3,\quad F_1 = 5,\quad F_2 = 17,\ \ldots$

Z.z. : $\prod_{k=0}^{n-1} F_k = F_n - 2$, $n \geq 1$ (*)

Beweis per Induktion :

IA: für n=1 gilt: $F_0 = F_1 - 2 = 3$ $\Rightarrow$ IV: (*)

IB: n=n+1: $\prod_{k=0}^{n} F_k = F_{n+1} - 2$

IS: $\prod_{k=0}^{n} F_k = (\prod_{k=0}^{n-1} F_k) \cdot F_n \overset{IV}{=} (F_n - 2) \cdot F_n \overset{Def}{=} (2^{2^n} + 1 - 2) \cdot (2^{2^n} + 1) = 2^{2^n+1} - 1 = 2^{2^n+1} + 1 - 2 = F_{n+1} - 2$

3. Beweis mithilfe der Eulerschen Phi-Funktion

- Def. **Phi-Funktion :**

$$\phi(n) := |\{ a \in N \mid 1 \leq a \leq n \ \wedge \ ggT(a, n) = 1 \}| \longrightarrow p \in P: \ \phi(p) = p-1$$

3. Beweis mithilfe der Eulerschen Phi-Funktion

- Def. **Phi-Funktion :**

$$\phi(n) := |\{ a \in N \mid 1 \leq a \leq n \ \wedge \ ggT(a, n) = 1 \}| \longrightarrow \quad p \in P: \ \phi(p) = p-1$$

- Der Wert der Phi-Funktion lässt sich für jedes $\mathbf{n \in N}$ aus dessen Primfaktorzerlegung berechnen :

$$\phi(n) := \prod_{p|n} p^{k-1} \cdot (p-1)$$

3. Beweis mithilfe der Eulerschen Phi-Funktion

- Def. Phi-Funktion :

$$\phi(n) := |\{ a \in N \mid 1 \leq a \leq n \ \wedge \ ggT(a, n) = 1 \}| \longrightarrow \quad p \in P: \ \phi(p) = p-1$$

- Der Wert der Phi-Funktion lässt sich für jedes **$n \in N$** aus dessen Primfaktorzerlegung berechnen :

$$\phi(n) := \prod_{p|n} p^{k-1} \cdot (p-1)$$

- Beispiel :

für 72 gilt : $\phi(72) = 24$ und $72 = 3^2 \cdot 2^3$

$$\phi(72) := 3^{2-1} \cdot (3-1) \cdot 2^{3-1} \cdot (2-1) = 3 \cdot 2 \cdot 4 \cdot 1 = 24$$

3. Beweis mithilfe der Eulerschen Phi-Funktion

- Def. **Phi-Funktion :**

$$\phi(n) := \prod_{p|n} p^{k-1} \cdot (p-1) \xrightarrow{\text{Beobachtung}} \prod_{p|n} p^{k-1} \cdot (p-1) > 1$$

3. Beweis mithilfe der Eulerschen Phi-Funktion

- Def. **Phi-Funktion :**

$\phi(n) := \prod_{p|n} p^{k-1} \cdot (p-1)$ $\xrightarrow{\text{Beobachtung}}$ $\prod_{p|n} p^{k-1} \cdot (p-1) > 1$ Beispiel: $n=4=2^2$: $\phi(4) = 2^{2-1} \cdot (2-1) = 2$

3. Beweis mithilfe der Eulerschen Phi-Funktion

- Def. **Phi-Funktion :**

$$\phi(n) := \prod_{p|n} p^{k-1} \cdot (p-1) \xrightarrow{\text{Beobachtung}} \prod_{p|n} p^{k-1} \cdot (p-1) > 1$$

Annahme : Es gibt endlich viele Primzahlen $\{p_1, \dots, p_r\}$ . . .

3. Beweis mithilfe der Eulerschen Phi-Funktion

- Def. **Phi-Funktion :**

$$\phi(n) := \prod_{p|n} p^{k-1} \cdot (p-1) \xrightarrow{\text{Beobachtung}} \prod_{p|n} p^{k-1} \cdot (p-1) > 1 \quad (1)$$

Annahme : Es gibt endlich viele Primzahlen $\{p_1, \ldots, p_r\}$ *. . .*

Beweis :

Sei $\mathbf{n := p_1 \cdot p_2 \cdot \ldots \cdot p_r}$ $\Rightarrow$ $\phi(n) = 1$ $\Rightarrow$ wegen (1) 

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Mersenne-Zahl** : $2^n - 1$, für $n \geq 0$

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Mersenne-Zahl** : $2^n - 1$, für $n \geq 0$
- Def. **Primkörper** :

  Endlicher Körper $\mathbb{Z}_p$ mit **p** Elementen, wobei **p** eine Primzahl ist, also $Z_p = \{0, .. , p-1\}$

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Mersenne-Zahl** : $2^n - 1$, für $n \geq 0$

- Def. **Primkörper** :

  Endlicher Körper $\mathbb{Z}_p$ mit **p** Elementen, wobei **p** eine Primzahl ist, also $Z_p = \{0, .. , p-1\}$

- Def. **Gruppe** :

  Gruppe $(G, \circ)$ Menge von Elementen zusammen mit einer Verknüpfung, die je zwei Elementen der Menge ein drittes Element derselben Menge zuordnet und die Gruppenaxiome erfüllt.

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Mersenne-Zahl** : $2^n - 1$, für $n \geq 0$

- Def. **Primkörper** :

  Endlicher Körper $\mathbb{Z}_p$ mit **p** Elementen, wobei **p** eine Primzahl ist, also $Z_p = \{0, .. , p-1\}$

- Def. **Gruppe** :

  Gruppe (G, ◦) Menge von Elementen zusammen mit einer Verknüpfung, die je zwei Elementen der Menge ein drittes Element derselben Menge zuordnet und die Gruppenaxiome erfüllt.

- Def. **Elementordnung** :

  Unter der Ordnung eines Gruppenelementes **g** einer Gruppe (G, ◦) versteht man die kleinste natürliche Zahl **n>0**, für die $\mathbf{g^n = e}$ gilt, wobei **e** das neutrale Element der Gruppe ist.

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Mersenne-Zahl** : $2^n - 1$, für $n \geq 0$
- Def. **Primkörper** :

  Endlicher Körper $\mathbb{Z}_p$ mit **p** Elementen, wobei **p** eine Primzahl ist, also $\mathbb{Z}_p = \{0, .. , p-1\}$

- Def. **(multiplikative) Gruppe (G, ·)** :

  Menge von Elementen zusammen mit Multiplikation als Verknüpfung, die je zwei Elementen der Menge ein drittes Element derselben Menge zuordnet und die Gruppenaxiome erfüllt.

- Def. **Ordnung eines Gruppenelementes** :

  Kleinste natürliche Zahl **n>0**, für die $\mathbf{g^n = e}$ gilt (**e := neutr. Element)**

- Def. **Satz von Lagrange (Spezialfall)** :

  Wenn $\mathbf{U = \{a, a^2, \ldots, a^n\}}$ eine zyklische Untergruppe von G ist, dann gilt: $\mathbf{n \mid |G|}$

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Mersenne-Zahl** : $2^n - 1$, für $n \geq 0$

- Def. **Primkörper** :

  Endlicher Körper $\mathbb{Z}_p$ mit **p** Elementen, wobei **p** eine Primzahl ist, also $\mathbb{Z}_p = \{0, .. , p-1\}$

- Def. **(multiplikative) Gruppe (G, ·)** :

  Menge von Elementen zusammen mit Multiplikation als Verknüpfung, die je zwei Elementen der Menge ein drittes Element derselben Menge zuordnet und die Gruppenaxiome erfüllt.

- Def. **Ordnung eines Gruppenelementes** :

  Kleinste natürliche Zahl **n>0**, für die $\mathbf{g^n = e}$ gilt (**e := neutr. Element**)

- Def. **Satz von Lagrange (Spezialfall)** :

  Wenn $\mathbf{U = \{a, a^2, \ldots, a^n\}}$ eine zyklische Untergruppe von G ist, dann gilt: $\mathbf{n \mid |G|}$

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Elementordnung :** Kleinste natürliche Zahl **n>0**, für die $g^n = e$ gilt (**e := neutr. Element**)
- Def. **Lagrange :** Wenn $U = \{a, a^2, \ldots, a^n\}$ eine zyklische Untergruppe von G ist, dann gilt: **n | |G|**

*Annahme : Es gibt endlich viele Primzahlen und **p** ist die größte Primzahl …*

*Beweisidee : Wir betrachten die Zahl $2^p - 1$ und zeigen, dass jeder Primteiler **q** von 2^p-1 größer als **p** ist*

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Elementordnung :** Kleinste natürliche Zahl **n>0**, für die $\mathbf{g^n = e}$ gilt (**e := neutr. Element**)
- Def. **Lagrange :** Wenn $\mathbf{U = \{a, a^2, \ldots, a^n\}}$ eine zyklische Untergruppe von G ist, dann gilt: **n | |G|**

*Annahme : Es gibt endlich viele Primzahlen und **p** ist die größte Primzahl …*

*Beweisidee : Wir betrachten die Zahl $\mathbf{2^p - 1}$ und zeigen, dass jeder Primteiler **q** von 2^p-1 größer als **p** ist*

Beweis :

1. Sei q Primteiler von 2^p-1
2. $\Rightarrow (G, \cdot) = (\mathbb{Z}_q \backslash \{0\}, \cdot) = \{1, \ldots, q-1\}$
3. $\Rightarrow$ e = 1
4. $\Rightarrow$ |G| = q-1

$\Rightarrow$

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Elementordnung :** Kleinste natürliche Zahl **n>0**, für die $\mathbf{g^n = e}$ gilt (**e := neutr. Element**)
- Def. **Lagrange :** Wenn $\mathbf{U = \{a, a^2, \ldots, a^n\}}$ eine zyklische Untergruppe von G ist, dann gilt: **n | |G|**

*Annahme : Es gibt endlich viele Primzahlen und **p** ist die größte Primzahl …*

*Beweisidee : Wir betrachten die Zahl **$2^p - 1$** und zeigen, dass jeder Primteiler **q** von **2^p-1** größer als **p** ist*

Beweis :

1. Sei q Primteiler von 2^p-1
2. $\Rightarrow (G, \cdot) = (\mathbb{Z}_q \backslash \{0\}, \cdot) = \{1, \ldots, q-1\}$
3. $\Rightarrow$ e = 1
4. $\Rightarrow$ |G| = q-1

$\Rightarrow$

(1.) $\Rightarrow$ $2^p \pmod q = 1 \pmod q$

4. Beweis mithilfe der Mersenne-Zahlen

- Def. Elementordnung : Kleinste natürliche Zahl **n>0**, für die $\mathbf{g^n = e}$ gilt (**e := neutr. Element**)
- Def. Lagrange : Wenn $\mathbf{U = \{a, a^2, \ldots, a^n\}}$ eine zyklische Untergruppe von G ist, dann gilt: **n | |G|**

*Annahme : Es gibt endlich viele Primzahlen und **p** ist die größte Primzahl …*

*Beweisidee : Wir betrachten die Zahl $\mathbf{2^p - 1}$ und zeigen, dass jeder Primteiler **q** von $\mathbf{2^p-1}$ größer als **p** ist*

Beweis :

1. Sei q Primteiler von 2^p-1
2. $\Rightarrow (G, \cdot) = (\mathbb{Z}_q \backslash \{0\}, \cdot) = \{1, \ldots, q-1\}$
3. $\Rightarrow$ e = 1
4. $\Rightarrow$ |G| = q-1

$\Rightarrow$

(1.) $\Rightarrow$ $2^p \pmod q = 1 \pmod q$

(E) $\Rightarrow$ 2 hat die Ordnung **p** in G

4. Beweis mithilfe der Mersenne-Zahlen

- Def. Elementordnung : Kleinste natürliche Zahl **n>0**, für die $\mathbf{g^n = e}$ gilt (**e := neutr. Element**)
- Def. Lagrange : Wenn $\mathbf{U = \{a, a^2, \ldots, a^n\}}$ eine zyklische Untergruppe von G ist, dann gilt: **n | |G|**

*Annahme : Es gibt endlich viele Primzahlen und **p** ist die größte Primzahl …*

*Beweisidee : Wir betrachten die Zahl **2^p - 1** und zeigen, dass jeder Primteiler **q** von **2^p-1** größer als **p** ist*

Beweis :

1. Sei q Primteiler von 2^p-1
2. $\Rightarrow (G, \cdot) = (\mathbb{Z}_q \backslash \{0\}, \cdot) = \{1, \ldots, q-1\}$
3. $\Rightarrow$ e = 1
4. $\Rightarrow$ |G| = q-1

$\Rightarrow$

(1.) $\Rightarrow$ $2^p \pmod q = 1 \pmod q$

(E) $\Rightarrow$ 2 hat die Ordnung **p** in G

$\Rightarrow$ U = $\{2^p, 2^{p*2}, \ldots\}$ ist zykl. Untergruppe mit p als kleinste natürliche Zahl

4. Beweis mithilfe der Mersenne-Zahlen

- Def. **Elementordnung :** Kleinste natürliche Zahl **n>0**, für die $\mathbf{g^n = e}$ gilt (**e := neutr. Element**)
- Def. **Lagrange :** Wenn $\mathbf{U = \{a, a^2, \ldots, a^n\}}$ eine zyklische Untergruppe von G ist, dann gilt: **n | |G|**

*Annahme : Es gibt endlich viele Primzahlen und **p** ist die größte Primzahl …*

*Beweisidee : Wir betrachten die Zahl **$2^p - 1$** und zeigen, dass jeder Primteiler **q** von **2^p-1** größer als **p** ist*

Beweis :

1. Sei q Primteiler von 2^p-1
2. $\Rightarrow (G, \cdot) = (\mathbb{Z}_q \backslash \{0\}, \cdot) = \{1, \ldots, q-1\}$
3. $\Rightarrow$ e = 1
4. $\Rightarrow$ |G| = q-1

$\Rightarrow$

(1.) $\Rightarrow$ $2^p \pmod q = 1 \pmod q$

(E) $\Rightarrow$ 2 hat die Ordnung **p** in G

$\Rightarrow$ U = $\{2^p, 2^{p*2}, \ldots\}$ ist zykl. Untergruppe mit p als kleinste natürliche Zahl

(L) $\Rightarrow$ p | |G| $\Rightarrow$ p | q-1 $\Rightarrow$ p < q ↯