Einiges über Primzahlen

Primzahlen: 2, 3, 5, ...

Primzahlen = „Bausteine der Zahlen",

denn: Jede Zahl 1, 2, 3, 4, 5, ... eindeutig(!) als Produkt von Primzahlen darstellbar. Etwa

$8 = 2 \cdot 2 \cdot 2$, $12 = 3 \cdot 2 \cdot 2$,

$100 = 10 \cdot 10 = 2 \cdot 5 \cdot 2 \cdot 5$

$= 2 \cdot 2 \cdot 5 \cdot 5$.

Leichte Beobachtung: Es gibt unendlich viele Primzahlen, denn.

Zu einer endlichen Menge von Primzahlen $p_1, \dots, p_n$ bilden wir

$$p_1 \cdot \dots \cdot p_n + 1.$$

Das muß keine Primzahl sein, hat aber eine Faktorisierung.

In dieser Faktorisierung kommt keines der p_i's vor. (Warum?!)

Also muß es weitere Primzahlen zu den $p_1, \dots, p_n$ geben.

Faktorisierungsproblem: Eingabe $n \in \mathbb{N}$.

Ausgabe: Faktorisierung von n in

Primfaktoren $n = p_1^{e_1} \cdot \ldots \cdot p_m^{e_m}$,

Exponenten $e_i \geq 1$.

Genau $e_i \leq \log n$

Algorithmen in

$$e^{\sqrt{\ln n \cdot (\ln \ln n)}}$$

Neu nicht effizient bekannt.

$$= e^{\frac{\ln \ln n}{\ln \ln n} \cdot \sqrt{\ln n (\ln \ln n)}}$$

$$= e^{\sqrt{\frac{\ln n}{\ln \ln n}}}$$

Nicht als opp-hard bekannt

$$= \ln n^{\sqrt{\frac{n}{\ln n}}}$$

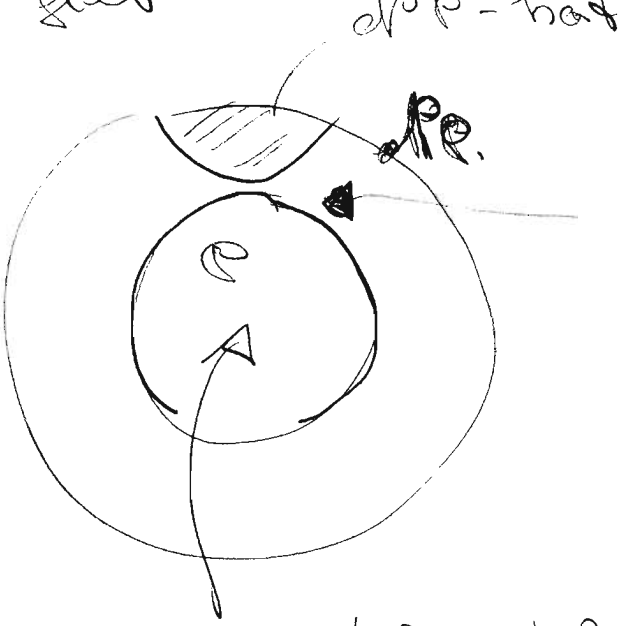
Entspricht $n^{n^{1/2-\varepsilon}} \geq n^{n^{1/2-\varepsilon}} \geq 2^{n^{1/2-\varepsilon}}$.

$\ln n$ = Logarithmus zu Basis e.

Primzahlproblem: Eingabe n,
ist n Primzahl? → Ja
→ Nein.

Aufgabe: Effizient gelöst: $\exists a, b \in \mathbb{N}$, $a \geq 2$ $n = a^b$
für $a, b \in \mathbb{N}$. Wie groß kann b maximal werden?

Es gibt



Faktorisierung effizient
⇒ Primzahl effizient.

Ein erster randomisierter (!)

Algorithmus:

Randomisierter Algorithmus.

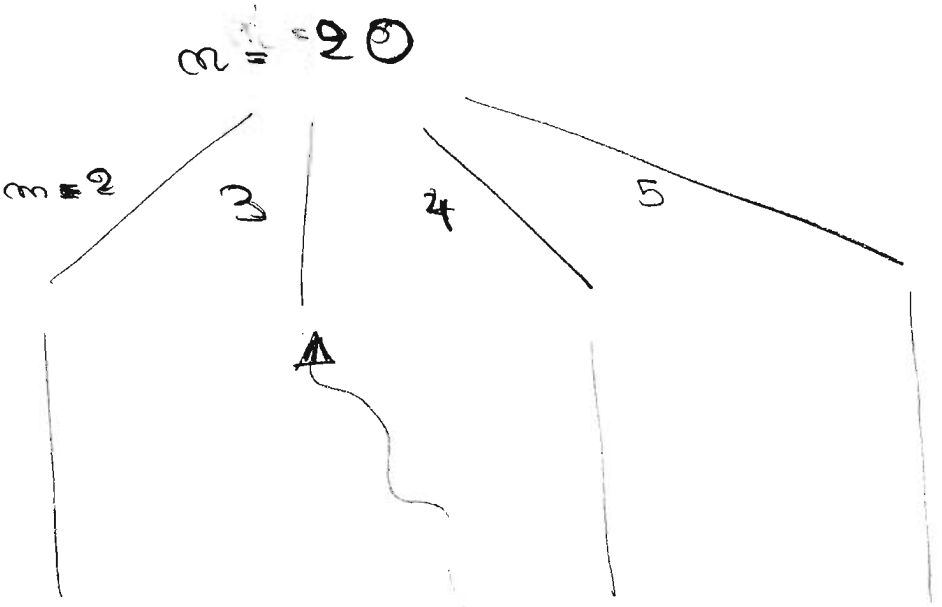
Eingabe: n

Wähle zufällig $2 \leq m \leq \sqrt{n}$

Teste, ob m ein Teiler von n ist

Ausgabe: Keine Primzahl, wenn $m \mid n$. sonst: Vielleicht Primzahl

$m \mid n$: Teilt.



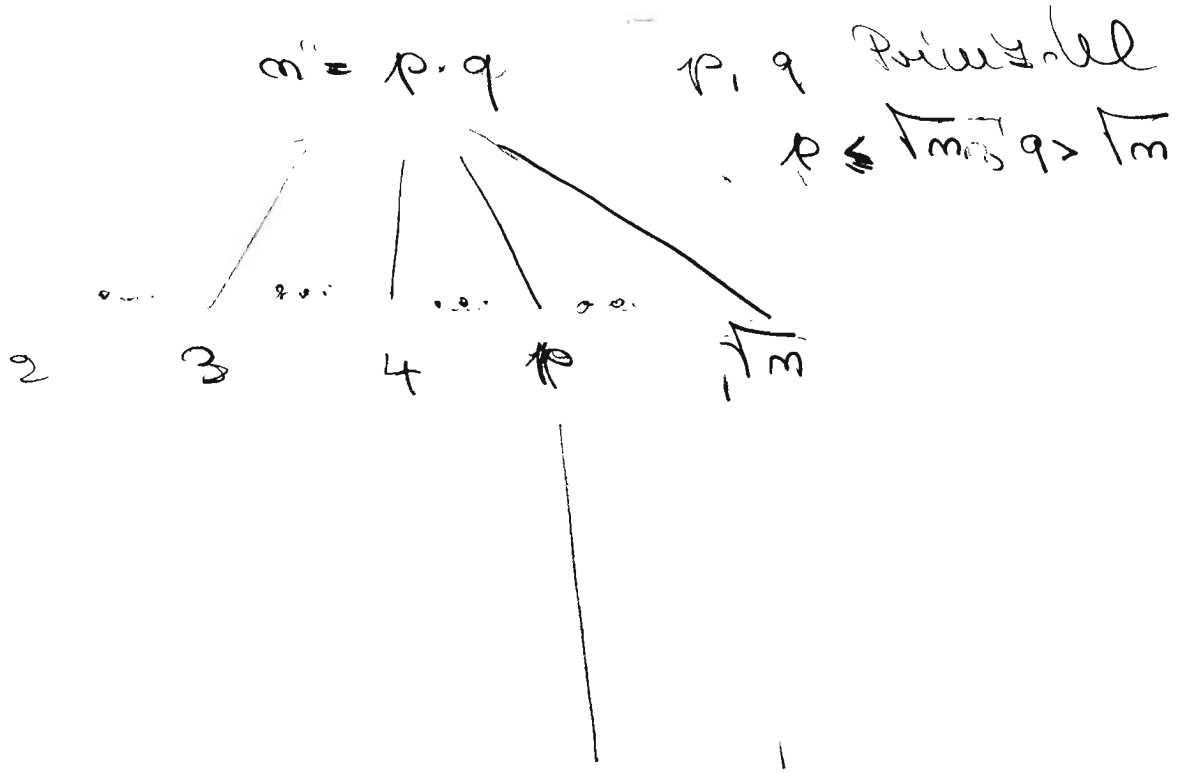
w-keit falsch $= 1/4 = 1 \cdot \frac{1}{4}$

W-keit 2-mal falsch $\frac{1}{15}$

W-keit k-mal falsch $\frac{1}{2^k} \to 0$

Dazu: k unabhängige Läufe.

Also zum Beispiel



W-keit $\approx \frac{1}{\sqrt{m}} \ll \frac{1}{\log m}$

1 - keine Lösung: $1 - \frac{1}{\sqrt{n}} \to 1$ für $n \to \infty$.

k - mal Lösung $\left(1 - \frac{1}{\sqrt{n}}\right)^k \leq e^{-\frac{1}{\sqrt{n}} k} \to 0$

wenn $k \gg \sqrt{n}$,

etwa $k = n^{\frac{3}{4}}$.

Aufgabe

Gebe eine Abschätzung

von $\left(1 - \frac{1}{\sqrt{n}}\right)^k$ von unten für

$k \ll \sqrt{n}$. Etwa mit dem Binomialsatz

$$\left(1 - \frac{1}{\sqrt{n}}\right)^k = 1 - \binom{k}{1} \cdot \frac{1}{\sqrt{n}} + \binom{k}{2} \cdot \left(\frac{1}{\sqrt{n}}\right)^2 - \binom{k}{3} \cdot \left(\frac{1}{\sqrt{n}}\right)^3 + \ldots$$

Man sieht vor $\gg \sqrt{n}$ Läufe

gebe uns noch gute Wahrscheinlichkeit

die richtige Antwort. ($\sqrt{n} = n^{1/2}$

$= 2^{\frac{1}{2}\log n} = \log n^{\frac{1}{2}\frac{\log n}{\log\log n}} \geq (\log n)^{(\log n)^{1-\varepsilon}}$

entspricht $n^{(n^{1-\varepsilon})}$)

Antwort: „Keine Primzahl" immer richtig, m ist Input.

Input müssen dürfen gesagt sein!

Antwort „Primzahl" kann mit W-keit $1-\frac{1}{\sqrt{m}}$ falsch sein.

$\Updownarrow$

Es gibt Inputs, bei denen das so ist. Bei Primzahlen ist die Antwort richtig.

Ziel: Für alle Inputs m, die keine Primzahl sind, soll sein: W-keit Antwort Primzahl sehr klein $\leq \frac{1}{m}$ evtl. $\leq \frac{1}{2^m}$ ...

Dazu mehr Fragen bei nicht prim.

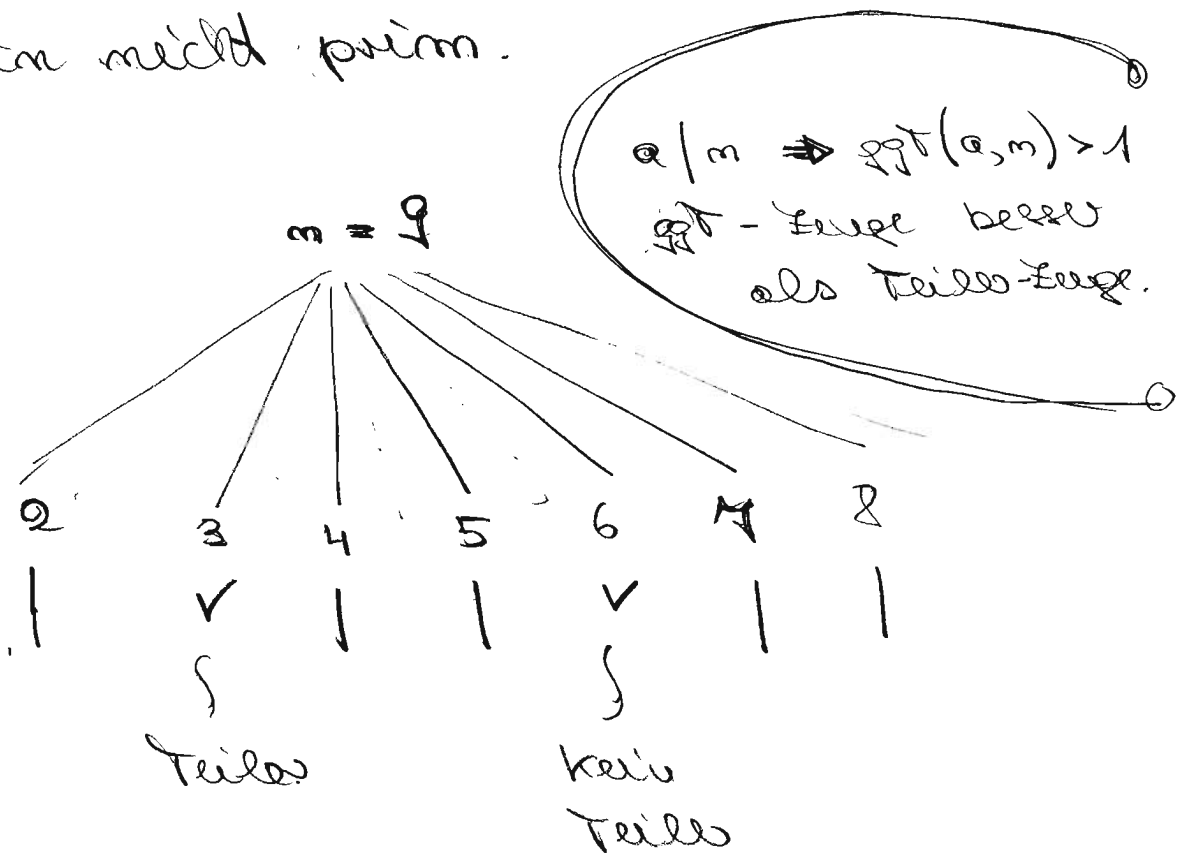
Sei immer n unsere Eingabe.

Der ggT-Test:

1. Wähle $1 < a < n$ zufällig

2. Teste $ggT(a,n) = 1$. Ja, prim,

nein nicht prim.



Hoffentlich $n = p \cdot q$, p, q prim,

$p, q \approx \sqrt{n}$ ...

Immer gilt: Ist $\operatorname{ggT}(a,m) = 1$

$\Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$, denn

$a^1, a^2, a^3, \dots, a^k = 1$, $ba^1, ba^2, \dots, ba^k$, $b \notin \{a^1, \dots, a^k\}$

Alle verschieden — Alle verschieden, weg. b^{-1}.

Falls z noch nicht e-fgBt.

$\dots \quad za^1, za^2, \dots, za^k \qquad a, b, \dots, z \in \mathbb{Z}_m^*$

Alle verschieden

Also $k \mid \varphi(m) = |\mathbb{Z}_m^*|$, also

$a^1, \dots, a^k = 1$, $a^{k+1} = a, \dots, a^{2k} = 1$,
$\dots a^{lk+1}, \dots, a^{lk+k} = a^{\varphi(m)} = 1$

$a^{\varphi(m)} = 1 \bmod m$.

Also m Primzahl, dann $\varphi(m) = m-1$

dann $a^{m-1} \equiv 1 \pmod m$ für $1 \le a < m$.

$\Leftrightarrow$ a nicht Vielfaches von m.

Fermat Zeuge

$a^{m-1} \not\equiv 1 \bmod m$.

Ist effizient(?) testbar:

$m-1 = \sum a_i \cdot b_i$

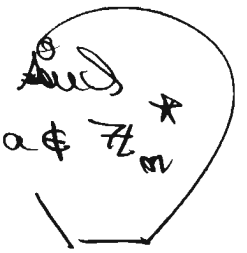
Teiler Zeuge ist ggT Zeuge.

ggT-Zeuge ist Fermat Zeuge,

denn $ggT(a,m) = d \neq 1$,

dann gilt für alle m $d \mid a^m$

aber $d \nmid 1$, also $a^{m+1} \neq 1$.



Wichtige Beobachtung:

Ist $a \in \mathbb{Z}_n^*$ ein Fermat-Zeuge,

dann gibt es $\geq \frac{n-1}{2}$ viele

Fermat-Zeugen unter $1, \ldots, n-1$.

Beweis.

Jedes $b \in \mathbb{Z}_n^*$ ist kein Fermat-

Zeuge.

Wie viele es in $\mathbb{Z}_m^*$ gibt? φ!

Wir betrachten die Fermat-Zeugen im $\mathbb{Z}_m^*$: ( ) D.h. $c^{m-1} = 1 \pmod m$

- Eines ist 1.
- Sind b, c solche, dann

$$(bc)^{m-1} \bmod m = \left(b^{m-1} \cdot c^{m-1}\right) \bmod m$$

$$= \underbrace{\left(b^{m-1} \bmod m\right)}_{=1} \cdot \underbrace{\left(c^{m-1} \bmod m\right)}_{=1} = 1 \cdot 1 = 1.$$

- Ist b ein solcher, dann auch b^{-1}, denn $b^{-1} = b^{m-2} \pmod m$,

$$\left(b^{m-2}\right)^{m-1} = \underbrace{\left(b^{m-1}\right)^{m-2}}_{=1} \bmod m.$$

Sei $NF \subseteq \mathbb{Z}_n^*$ die Menge (Untergruppe) der Nicht-Zeugen.

Für unseren Zeugen a gilt

$$|a \cdot NF| = |NF| \text{ und}$$

$$a \cdot NF \cap NF = \emptyset,$$

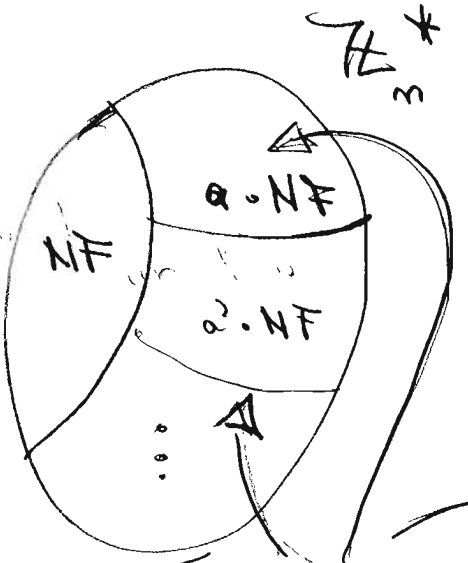
Lagrange:
Elemente in Untergruppe teilt # Elemente in Gruppe.

also für $b \in NF$

$$(a \cdot b)^{n-1} = a^{n-1} \underbrace{b^{n-1}}_{1} \bmod n$$

$$= a^{n-1} \bmod n \neq 1.$$

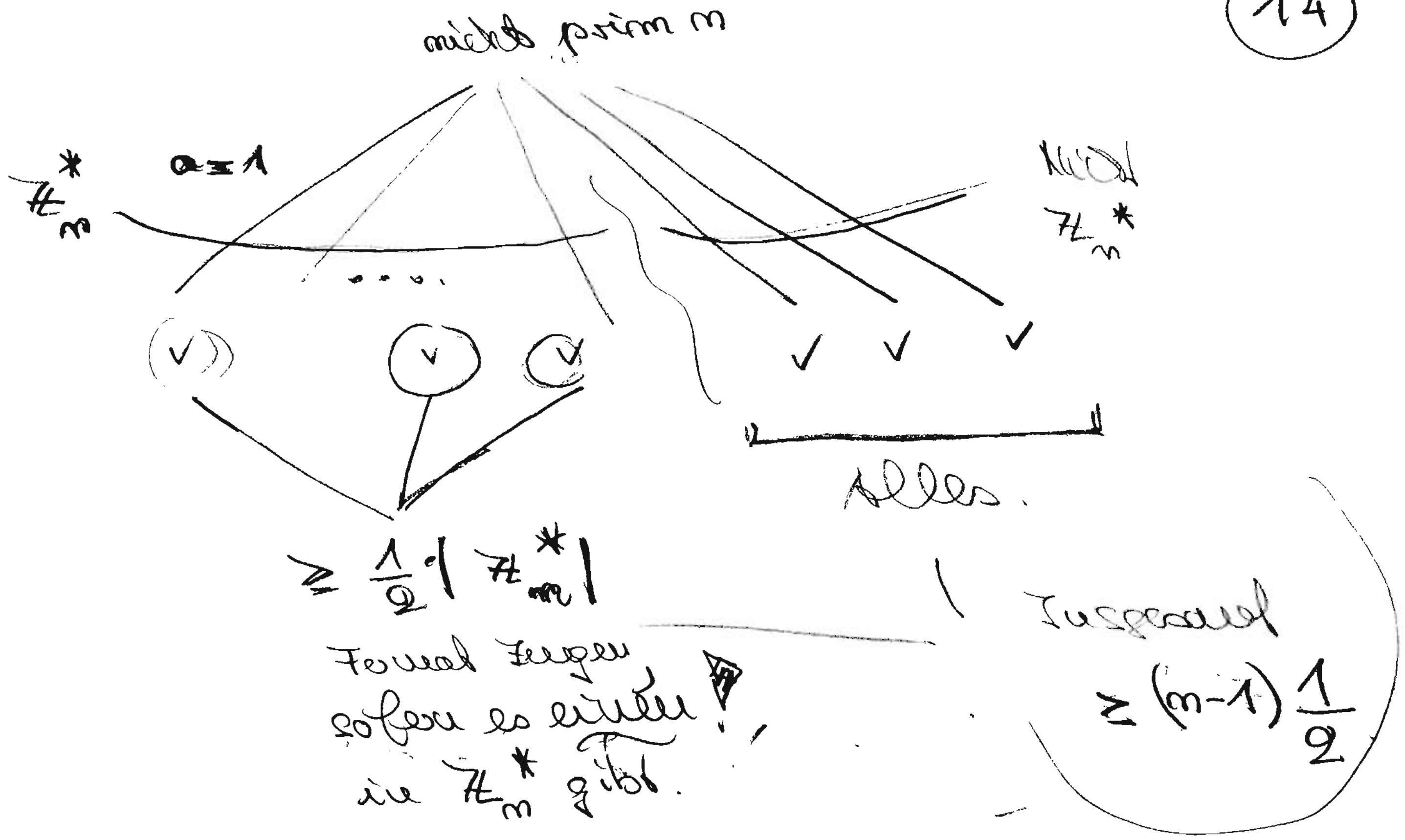
Alle $a \cdot b$ verschieden für $b \in NF$



sind also fernab Zeugen.

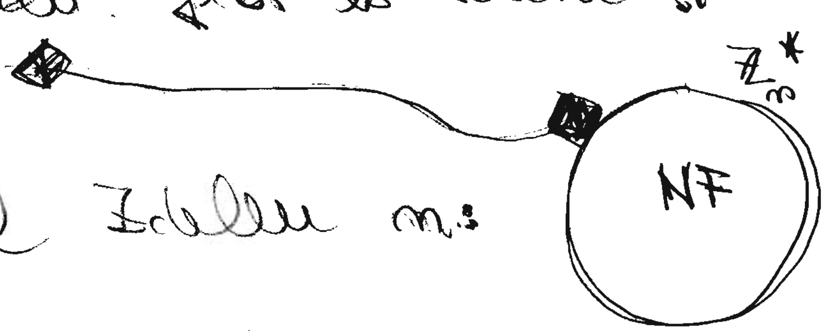
also $|NF| \leq \frac{1}{2} |\mathbb{Z}_n^*|$, es gibt

es einen fernab Zeugen in $\mathbb{Z}_n^*$ gibt.



Also W-keit richtig $\geq 1/2$.

Das einzige Problem sind Zahlen, die keinen Fermat-Zeugen in $\mathbb{Z}_n^*$ haben. Gibt es solche?



Carmichael Zahlen n:

- n nicht prim
- $a^{n-1} \equiv 1 \pmod{n}$ für alle $a \in \mathbb{Z}_n^*$

kein Fermat Zeuge in $\mathbb{Z}_n^*$

Carmichael Zahlen

Fermat Zeuge = g^{n-1} - Zeuge.

↑ Nur das was nicht in $\mathbb{Z}_m^*$ ist!

Es gilt:

$561 = 3 \cdot 11 \cdot 17$

$\mathbb{Z}_{561}^* = 2 \cdot 10 \cdot 16 = 320$

ist eine Carmichael Zahl.

Dazu zunächst eine allgemeine Überlegung (Chinesischer Restsatz).

Ist $m = a \cdot b$, $\operatorname{ggT}(a,b) = 1$.

Wir behaupten: $= a \cdot b - 1$

$$\mathbb{Z}_m = \{0, \dots, m-1\}$$ $a \cdot b$ Elemente

verhält sich wie (ist isomorph zu)

$$\mathbb{Z}_a \times \mathbb{Z}_b = \{(0,0), \dots, (a-1, b-1)\}.$$

$a \cdot b$ Elemente.

mit der Entsprechung (Isomorphie)

$$c \longmapsto (c \bmod a,\ c \bmod b)$$

$c \in \mathbb{Z}_m$ | $c \bmod a \in \mathbb{Z}_a$ | $c \bmod b \in \mathbb{Z}_b$

Beispiel $a = 3$, $b = 2$

Rechne auf $\mathbb{Z}_a \times \mathbb{Z}_b$ komponentenweise aus!

$\mathbb{Z}_6^*$

$0 \rightsquigarrow (0,0)$ | $3 \rightsquigarrow (0,1)$

$1 \rightsquigarrow (1,1)$ | $4 \rightsquigarrow (1,0)$

$2 \rightsquigarrow (2,0)$ | $5 \rightsquigarrow (2,1)$

$\mathbb{Z}_6^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_2^*$

Umkehrung mod $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

$(c,d) \mapsto c \cdot d \bmod 6$

Auch die Operation ist übertragbar!!

Erst mod $\mathbb{Z}_3 \times \mathbb{Z}_2$, dann rechnen.

$(1+1) \bmod 6 = 2$

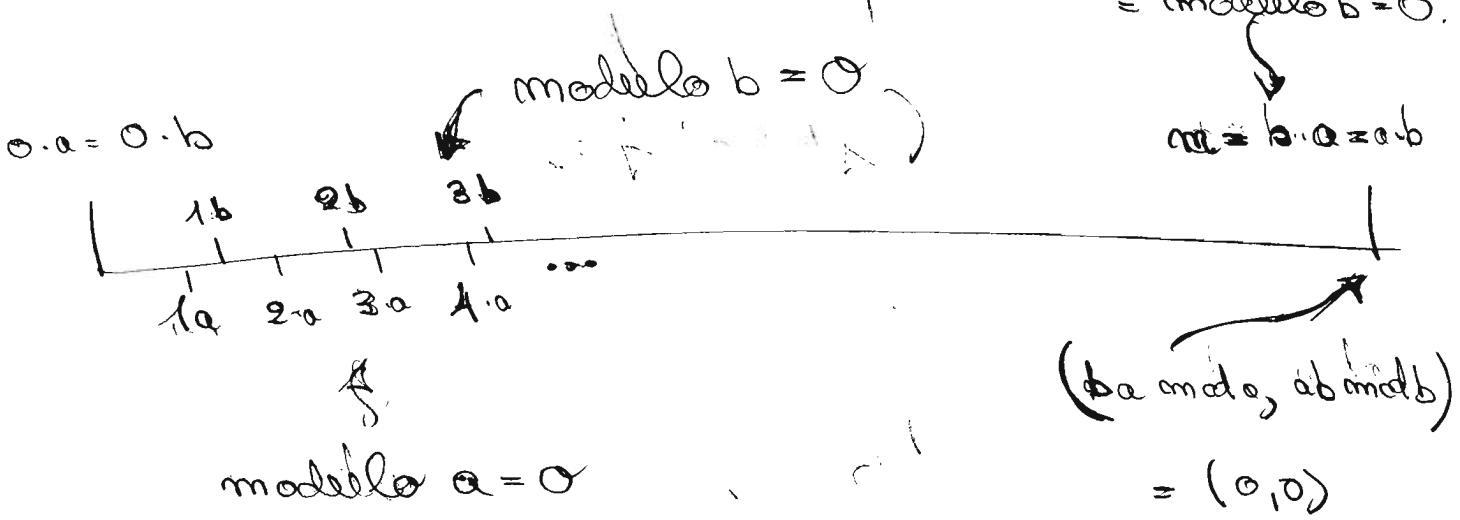
Rechne in $\mathbb{Z}_{61}$ dann mod $\mathbb{Z}_3 \times \mathbb{Z}_2$

$(1,1) + (1,1) \bmod (3,2) = ((1+1) \bmod 3,\ (1+1) \bmod 2) = (2,0)$

$2 \cdot 2 \bmod 6 = 4$

$(2,0) \cdot (2,0) \bmod (3,2) = (1,0)$

Wie zu beweisen?



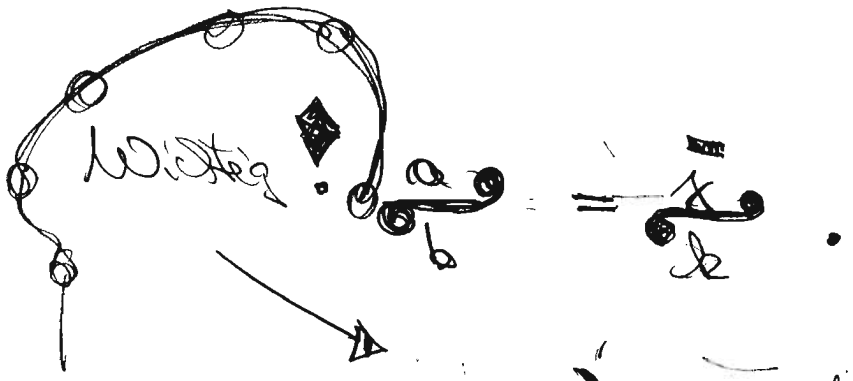
Es gilt m ist der erste Wert von allen Werten $1, 2, \dots, m$ mit

$$\text{modulo } a = \text{modulo } b = 0.$$

Betrachten $k \cdot a$ und $j \cdot b$ (alle anderen Werte kann das sowieso nicht in Frage kommen). Ist jetzt

$$k \cdot a = j \cdot b$$

ein Wert mit $\text{mod } a = \text{mod } b = 0$, dann



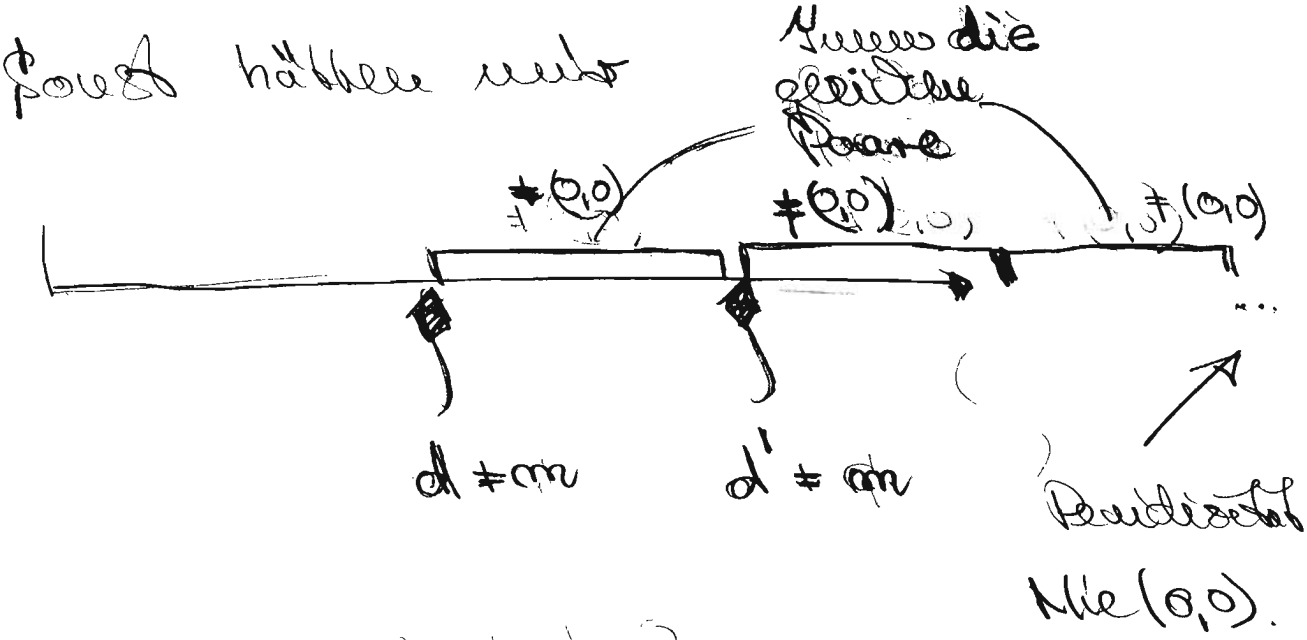
Da $ggT(a,b) = 1$ ist also $x = j \cdot a$, $k = j \cdot b$

Jetzt können wir weiter folgern

für $1 \leq d \neq d' \leq m$ ist

$$(d \bmod a, d' \bmod b)$$

$$\neq (d' \bmod a, d' \bmod b).$$



Also, die Abbildung

$$c \longmapsto (\underbrace{c \bmod a}_{\in \mathbb{Z}_a}, \underbrace{c \bmod b}_{\in \mathbb{Z}_b})$$

$\in \mathbb{Z}_m$ $\quad m = a \cdot b$, $\operatorname{ggT}(a,b) = 1$

ist bijektiv, da $\left| \mathbb{Z}_a \times \mathbb{Z}_b \right| = \underbrace{a \cdot b}_{= m} = \left| \mathbb{Z}_m \right|$.

Das Rechnen überträgt sich, da

$$(c+d) \bmod m \rightsquigarrow \big((c+d) \bmod m\big) \bmod a,\ \big((c+d) \bmod m\big) \bmod b\big)$$

Beweise $a, b \mid m$ ✍ $\rightsquigarrow$

$$= \big((c+d) \bmod a,\ (c+d) \bmod b\big)$$

$$= \big((c \bmod a, d \bmod b) + (d \bmod a, d \bmod b)\big) \bmod (a, b)$$

$\ldots \cdot b$, d.h. $\ldots$

Ebenso

$$(c \cdot d \bmod m) \rightsquigarrow (c \cdot d \bmod a,\ c \cdot d \bmod b)$$!

Umkehrung ist nicht (!)

$$(c,d) \mapsto (c \cdot d) \bmod m \quad ,$$

$\uparrow \quad \uparrow$

$\mathbb{Z}_a \quad \mathbb{Z}_b$ wegen $q = 0$ etwa,

vgl. Beispiel auf S. 16.

sondern kompliziertes.

Aber

$$\mathbb{Z}_m^* \cong \mathbb{Z}_a^* \times \mathbb{Z}_b^*$$

mittels

$$q \mapsto (q \bmod a,\ c \bmod b),$$

denn

$$\ggT(q, a \cdot b) = 1 \iff \ggT(c, a) = 1$$

$$\text{und } \ggT(c, b) = 1$$

$$(\text{da } 1 = \lambda q + \mu a b, \ldots)$$

Folgerung (Kongruenzgleichungssysteme, lösen)

Sind $a, a' \geq 0$ und x mit $\operatorname{ggT}(a,b) = 1$. Dann gibt das Gleichungssystem

$$x = d \bmod a$$
$$x = d' \bmod b$$

hat genau eine Lösung x mit $1 \leq x \leq a \cdot b$ (oder genau eine Lösung modulo $a \cdot b$).

Das Urbild von (d,d') unserer Bijektion $CH(c \bmod a, c \bmod b)$ ist die Lösung.

Effizient finden wir sie nicht.

Ebenso für mehrere $a, b, c, \ldots$ alle paarweise teilerfremd. Dann

$\mathbb{Z}_{a \cdot b \cdot c \cdots}$ isomorph zu $\mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c \cdots$

Gegenbeispiel

$a = b = 2$, dann $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$

$0 \mapsto (0,0)$ $\quad 2 \mapsto (0,0)$

$1 \mapsto (1,1)$ $\quad 3 \mapsto (1,1)$

Nicht mehr bijektiv.

Zu wenig Carmichael Ideal

$m = 561 = 3 \cdot 11 \cdot 17$. (Für alle $a \in \mathbb{Z}_m^*$ soll gelten $a^{m-1} \equiv 1 \bmod m$.

Wie sieht man das? Nun wie kennen $\mathbb{Z}_m$. Es ist wie

$$\mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{17}$$

Und $\mathbb{Z}_m^*$ ist isomorph zu

$$\mathbb{Z}_3^* \times \mathbb{Z}_{11}^* \times \mathbb{Z}_{17}^*$$

$$\updownarrow \qquad \updownarrow \qquad \updownarrow$$

$$1,2 \qquad 1,\dots,10 \qquad 1,\dots,16.$$

Nun gilt $m-1 = 560$

$2 \mid 560$, $10 \mid 560$, $16 \mid 560$.

$16 \cdot 35 = 560$.

Teilt.

Also gilt für $(c,d,e) \in \mathbb{Z}_3^* \times \mathbb{Z}_{11}^* \times \mathbb{Z}_{17}^*$

daß $(c,d,e)^{m-1} = (1,1,1) \bmod (3,11,17)$

Also gilt für $f \in \mathbb{Z}_m$ mit

$(f \bmod 3, f \bmod 11, f \bmod 17)$

$= (c,d,e)$,

daß $f^{m-1} = 1$ ist.

Also gilt das für alle $\ell \in \mathbb{Z}_m^*$.

Zusatz: Zum Fermat Zeugen
die reellen Rabin Zeugen.
Es gilt: Ist n Primzahl,
dann gilt für $1 \leq b < n$:
Ist $b^2 = 1 \bmod n$, dann

$$b = +1 \bmod n \quad \text{oder}$$

$$b = -1 \bmod n = (n-1) \bmod n.$$

Denn, ist $b \neq 1$ und $b \neq -1$ und
($b^2 = 1 \bmod n$)
($\bmod n$), dann ist

$$0 = \underbrace{b^2 - 1}_{=1} = \underbrace{(b+1)}_{\neq 0} \cdot \underbrace{(b-1)}_{\neq 0}$$

da $b \neq -1$ da $b \neq 1$

und $b+1$; $b-1$ teilen n, also nicht prim.

Algorithmus (Miller-Rabin)

Eingabe n.

1. n gerade, nicht prim.
2. a zufällig aus $1, \dots, n-1$.
3. $a^{n-1} \neq 1 \bmod n$, nicht prim (Fermat)
4. Dividiere alle 2er aus $n-1$ raus:

$$n-1 = 2^k \cdot l, \quad l \text{ ungerade.}$$

$k \leq \log n$

5. Betrachte

$$\rightarrow \left(a^l, a^{2l}, a^{2^2 l}, \dots, a^{2^k l} \right)$$

$= n-1$

Suche eine 1 in der Folge, so dass

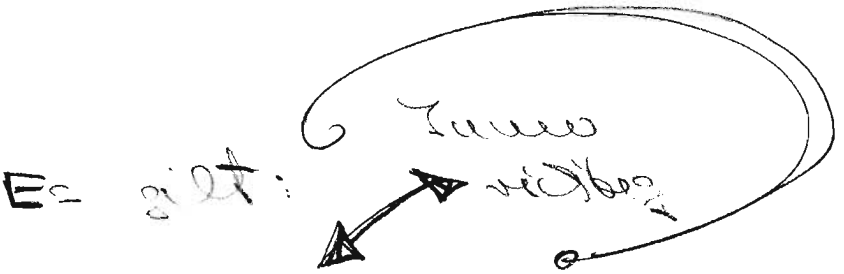
Der vorher wieder 1 mod n.

Dann nicht prim. (Miller-Rabin)

6. Hier Ausgabe, vermutlich prim.

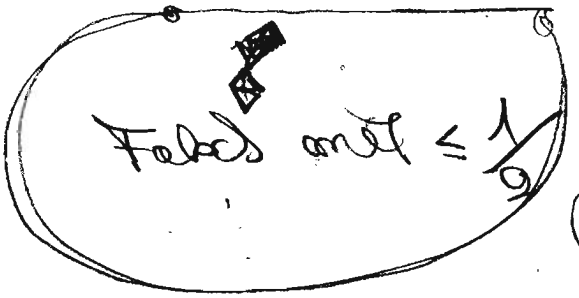
$\geq 1/2$

Es gibt:



n prim ⇒ keine prim. ✓

n nicht prim ⇒ keine nicht prim



mit Wahrscheinlichkeit $\geq 1/2$

(also prim mit $\leq 1/2$)

k-Läufe, dann Wahrscheinlichkeit nicht prim

$\leq \left(\frac{1}{2}\right)^k \to 0$ für $k = m$.

Das zeigen wir jetzt für alle

n, n nicht prim.

Ist n gerade, dann neg. 1. ✓

Ist $ggT(a,n) > 1$, dann klappt der

Fermat Test $\frac{1}{2}$. ✓

Also da a einfach auf $1, -, m-1$
ist, können wir die jetzt annehmen,
a einfach aus $\mathbb{Z}_m^*$.

Ein spezieller Sonderfall, $m = p^\alpha$, $\alpha > 1$ (p prim, $p \neq 2$)
(sogar deterministisch entscheidbar,
aber nicht so effizient.)

Zeigen, es gibt Fermat Zeugen
$b \in \mathbb{Z}_m^*$ (damit $\geq \frac{1}{2} |\mathbb{Z}_m^*|$ Fermat Zeugen).

Es tut's

$$b = 1 + p^{\alpha-1}.$$

Es ist $\operatorname{ggT}(p^\alpha, 1 + p^{\alpha-1}) = 1$

(alternativ $(1+p^{\alpha-1})(1+p^{\alpha-1})$
$= 1 - p^{(\alpha-1)2} = 1 - p^{\alpha+\alpha-2} = 1$
(also $\bmod n$))

Aber es gilt auch (alles modulo n)

$$b^{n-1} = \left(1 + p^{\alpha-1}\right)^{n-1}$$

Binomialsatz

$$= 1 + (n-1)\cdot p^{\alpha-1} + \text{Potenzen } \left(p^{\alpha-1}\right)^2, \left(p^{\alpha-1}\right)^3, \ldots$$

$$= 0 \pmod{n}$$

$$= 1 - p^{\alpha-1}$$

$n = p^{\alpha}$

$$= b^{-1} \neq 1 \bmod n, \text{ da}$$

$$b = 1 + p^{\alpha-1} \neq 1$$

$$< n-1$$

$$< n$$

Gilt das nicht sogar für $n = m^{\alpha}$ irgendein m $m \neq 2$.

Also $b \in \mathbb{Z}_n^*$ ist

Fermat Zeuge.

Jetzt der eigentliche Fall.

n hat ≥ 2 verschiedene Primfaktoren.

Wir schreiben

$$n = u \cdot v \quad , \quad \operatorname{ggT}(u,v) = 1.$$

u, v ungerade, da n ungerade.

Chinesischer Rest

$\mathbb{Z}_n^*$ ist isomorph $\mathbb{Z}_u^* \times \mathbb{Z}_v^*$

$$b \longmapsto (b \bmod u, \; b \bmod v).$$

Wir kürzen ab: $G = \mathbb{Z}_n^*$.

$$\varphi_m : G \to G$$
$$b \mapsto b^m$$

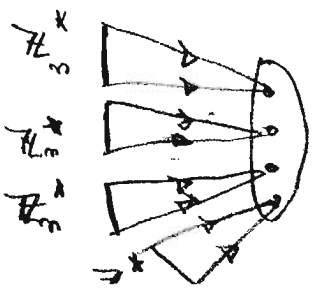
$u = \mathbb{Z}_u^*$,
$v = \mathbb{Z}_v^*$

Dann gilt: Jedes Element, das von φ_m getroffen wird, wird von der gleichen Anzahl b^1 getroffen.

- $1 = 1^m = \varphi_m(1)$.
- Ist $b^m = 1, b \neq 1$ und ist $\varphi_m(c) = c^m$, dann $\varphi_m(bc) = c^m$ und $bc \neq c$, da $c \neq 1$.
- $\left|\varphi_m^{-1}(1)\right| = \left|\varphi_m^{-1}(c^m)\right|$.

Gilt jedes $q \in \mathbb{P}$.

- Für unser $a \in \mathbb{Z}_m^*$ zufällig ist $\varphi_m(a) \in Q^m$ zufällig, aus Q^m.



$Q^m = \{b^m \bmod m \mid b \in \mathbb{Z}_m^*\}$

Ebenso

$$U^m = \{ c^m \bmod u \mid c \in \mathbb{Z}_u^* \}$$

$$V^m = \{ d^m \bmod v \mid d \in \mathbb{Z}_v^* \}$$

$m = u \cdot v$

Es ist auch Δ^m isomorph

zu $U^m \times V^m$.

$b^m \mapsto (b^m \bmod u, b^m \bmod v)$

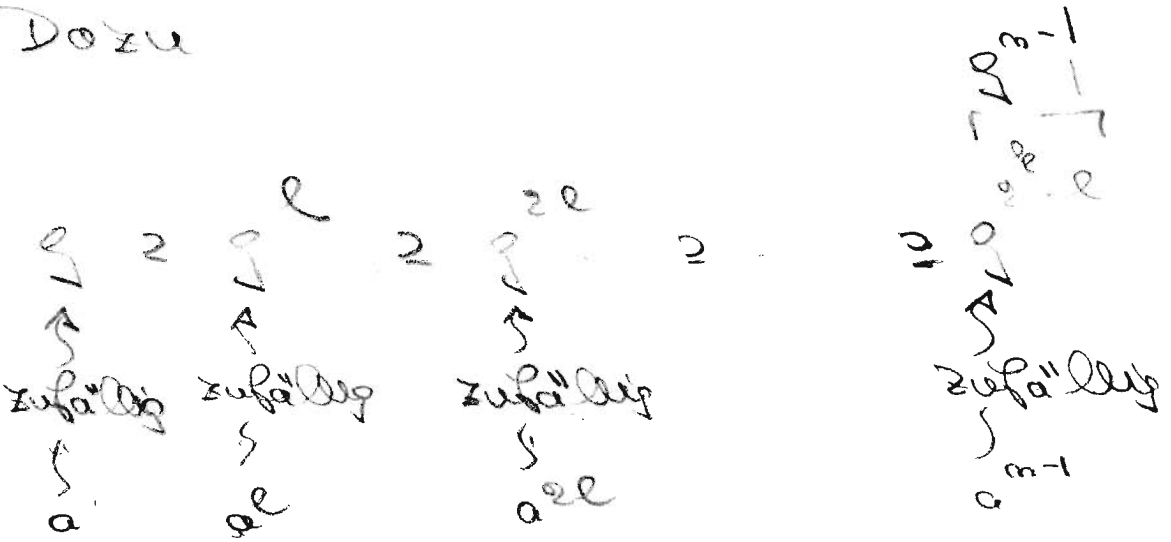
$c^m \bmod u$ $\quad$ $d^m \bmod v$

Nun zu dem Schritt 5 des Algorithmus.

$a^1, a^2, a^3, \ldots, a^{n-1}$

a teilerfremd zu $\mathbb{Z}_m^* = ?$

Dazu



und Isomorphie

$$\mathbb{Z}_u \times \mathbb{Z}_v \cong U^{\ell} \times V^{\ell} \cong U^{2\ell} \times V^{2\ell} \cong \dots \cong U^{n-1} \times V^{n-1}.$$

$\mathbb{Z}_u^{\times}$ $\mathbb{Z}_v^{\times}$

Ein Misserfolg: $U^{n-1} \neq \{1\}$ oder $V^{n-1} \neq \{1\}$,

dann $p^{n-1} \neq (1)$, also Fermat Test

und damit (wie immer) mit Wkeit $\geq 1/2$.

Restliche injektive Abbildung

$$1 \rightsquigarrow (1 \bmod u, 1 \bmod v) = (1,1).$$

Der Hauptfall wieder:

$$u^{n-1} = \{1\} \text{ und } v^{n-1} = \{1\}.$$

(denn $\zeta^{n-1} = \{1\}$, Fermat gilt nicht.)

wir haben jetzt

$$\{1\} \neq u^{\ell} \geq u^{2\ell} \geq \dots \geq u^{n-1} = \{1\}$$

$$\{1\} \neq v^{\ell} \geq v^{2\ell} \geq \dots \geq v^{n-1} = \{1\}.$$

Es ist $u^{\ell} \neq \{1\}$ und $v^{\ell} \neq \{1\}$,

denn $-1 \in u$ $(= \mathbb{Z}_u^*)$ $-1 \in v$ $(= \mathbb{Z}_v^*)$

$\llcorner$ $= u-1$ $\llcorner$ $= v-1$ $-1 \mapsto (-1,-1)$

und $(-1)^{\ell} = -1$, da ℓ ungerade

(alles modulo u und v). Und $-1 \neq 1$,

da $u, v \neq 2$.

Wir gehen jetzt von vorhin noch kürzer in umgekehrter Folgerung.

Wir finden die erste Stelle von rechts, an der

$$a^m \neq 1 \text{ oder } V^m \neq \{1\}$$

(oder beide)

Also $m = 2^\lambda \cdot \ell$ $0 \leq \lambda < k$

und $u^{2m} = \{1\}$, $V^{2m} = \{1\}$

und u^m, V^m wie gehabt.

Wir zeigen, daß beide Relationen Zeugen mod 5. mit W-Satz $\geq 1/2$ erfolgreich.

Es sei für unser zufälliges $a \in G$

$$a^{2m} = 1.$$

Die Behauptung (bezogen auf das vorliegende $a \in \mathbb{Z}_m^*$) ist nun, daß

$$a^m \neq 1 \text{ und } \neq -1$$

ist.

Nun, ein Unterfall: Ist $u^m = \overline{1}$ und $v^m \neq \overline{1}$ (oder umgekehrt).

Wie ist g^m? Es ist $-1 \notin g^m$,

denn mit einem Isomorphismus ist

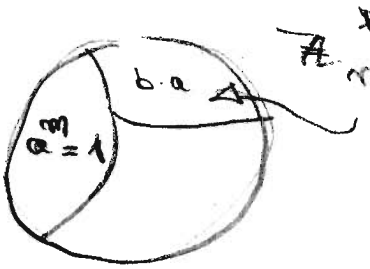
$$-1 \mapsto (-1, -1) \in \mathbb{Z}_u^* \times \mathbb{Z}_v^*,$$

also $-1 \notin g^m$, also $a^m \neq -1$,

immer, d.h. 10-teil = 1. Aber $a^m = 1$ ist möglich. Es gibt aber $b \in \mathbb{Z}_m^*$ mit $b^m \neq 1$, das sind mehr als die

Hälfte (da die Menge der $a \in \mathbb{Z}_n^*$

mit $a^m = 1$ eine Untergruppe bildet



$b^m \neq 1$, $a^m = 1$,
dann $(ba)^m \neq 1$

Lagrange - Satz).

Also hat mindestens die Hälfte $a \in \mathbb{Z}_n^*$

die Eigenschaft $a^m \neq 1$ ist $\geq 1/2$.

(-1 sowieso ausgeschlossen).

Schließlich noch: $u^m \neq \{1\}$,

und $v^m \neq \{1\}$.

Dann $\underbrace{|u^m|}_{=q}, \underbrace{|v^m|}_{=d} \geq 2$. Also

$|g^m| = q \cdot d \geq 4$

$g^m = u^m \cdot v^m$

Dann gibt die so-bekannte, daß

unter zufälligen a $a^m = 1$

erfüllt ist $\leq 1/4$. (Lagrange,)

beachte ganz g^m wird getroffen,

jedes Element gleichhäufig.)

Schließlich noch der Fall -1:

Ist $-1 \notin g^m$ dann ist alles gut.

Ist $-1 \in g^m$, dann ist -1 eines

von mindestens 4 Elementen

Es gibt mit 10-Koef $\leq 1/4$
auch (wieder Lagrange). Also
10-Koef 1 getroffen oder -1
getroffen

$$\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

Also mit $\geq \frac{1}{2}$ $a^m \neq 1, -1$
und Robin Hilbert erfolgreich.