§1 Allgemeines zu Kryptographie-Verfahren

§1.1 Grundlagen aus der elementaren Zahlentheorie / Gruppentheorie

Stichworte:

Def. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, g-adische Entw. / Binärentw.
Def. Gruppe / Ring / Körper, Teilbarkeit
Def. ggT, relativ prim / teilerfremd, PFZ
Eind. der PFZ $\rightsquigarrow$ Faktorisierungsproblem
ggT: Div. mit Rest / Eukl. Algo mit Erweiterung (↦ Bézout-El.)

1.1.1 Zahlen, Darstellung von Zahlen

Die Zahlbereiche $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sind aus den Grundvorlesungen bekannt. Bzgl. den Verknüpfungen + und · sind verschiedene Axiome erfüllt, die diese Zahlbereiche zu interessanten algebraischen Strukturen machen:

Halbgruppe	Gruppe	Ring	Körper
$(\mathbb{N},+), (\mathbb{N},\cdot)$			
$(\mathbb{Z},+), (\mathbb{Z},\cdot)$	$(\mathbb{Z},+,0)$	$(\mathbb{Z},+,\cdot)$	
$(\mathbb{Q},+), (\mathbb{Q},\cdot)$	$(\mathbb{Q},+,0), (\mathbb{Q}\setminus\{0\},\cdot,1)$	$(\mathbb{Q},+,\cdot)$	$(\mathbb{Q},+,\cdot)$
$(\mathbb{R},+), (\mathbb{R},\cdot)$	$(\mathbb{R},+,0), (\mathbb{R}\setminus\{0\},\cdot,1)$	$(\mathbb{R},+,\cdot)$	$(\mathbb{R},+,\cdot)$
$(\mathbb{C},+), (\mathbb{C},\cdot)$	$(\mathbb{C},+,0), (\mathbb{C}\setminus\{0\},\cdot,1)$	$(\mathbb{C},+,\cdot)$	$(\mathbb{C},+,\cdot)$

Weiter sind $\mathbb{Q}$ und $\mathbb{R}$ angeordnete Körper, d.h. es gibt eine Anordnungsrelation $\leq$, die sich mit +, · verträgt. Für $\mathbb{C}$ ist eine solche Anordnung nicht mehr möglich.

Wir erinnern an die Definitionen:

1.) • **Def.:** Eine Menge $H \neq \emptyset$ mit Verknüpfung $*: H \times H \to H$, $*(a,b) = a*b$ heißt Halbgruppe, falls $*$ assoziativ ist, d.h. $\forall a,b,c \in H: a*(b*c) = (a*b)*c$

2.) • **Def.:** Eine Halbgruppe $(G,*)$ heißt Gruppe, falls es ein neutrales Element $e \in G$ gibt (mit $e*g = g*e = g$ für alle $g \in G$), und falls zu jedem $g \in G$ ein inverses Element $h \in G$ existiert mit $g*h = e = h*g$ (schreiben dann auch g^{-1} oder $\frac{1}{g}$ oder $1/g$ oder $-g$).

3.) • **Def.:** Eine Gruppe $(G,*,e)$ heißt abelsch bzw. kommutativ, falls $\forall a,b \in G: a*b = b*a$.

4.) • **Def.:** Ein Ring $(R,+,\cdot)$ ist eine Menge $R \neq \emptyset$ und zwei Verknüpfungen $+$ und $\cdot$ so, dass $(R,+,0)$ eine Gruppe ist, $(R,\cdot,1)$ eine Halbgruppe mit neutr. El. 1, und so, dass die Distributivgesetze $(a+b)\cdot c = a\cdot c + b\cdot c$ und $c\cdot(a+b) = c\cdot a + c\cdot b$ gelten.

bedr. nur: Ring "mit 1" →

5) **Bem.:** Die Addition $+$ ist in einem Ring stets kommutativ.
Ein Ring heißt kommutativ, wenn die Multiplikation $\cdot$ kommutativ ist.
Soll der Nullring $R = \{0\}$ mit $1 = 0$ ausgeschlossen werden, fordert man zusätzlich noch $1 \neq 0$ in den Ringaxiomen.

6) • **Def.:** Die in einem Ring $(R,+,\cdot)$ bzgl. $\cdot$ invertierbaren Elemente heißen Einheiten. Die Menge der Einheiten in R wird mit R^* bezeichnet, d.h. also $R^* := \{a \in R;\ \exists\, b \in R: a\cdot b = 1 = b\cdot a\}$.
Damit ist $(R^*,\cdot,1)$ also eine Gruppe.

7.) • **Def.:** Ein Körper $(K,+,\cdot)$ ist ein kommutativer Ring mit $1 \neq 0$, für den $K^* = K \setminus \{0\}$ gilt.

Algebraische Strukturen dieser Art können wir auch in Teilmengen von $\mathbb{Z}$ auffinden und diese für kryptographische Anwendungen ausnutzen. Darum geht es in §1 dieser Vorlesung.

Dabei wird klar, dass die Anwendungen auch – teilweise – in beliebigen Gruppen / Ringen / Körpern möglich sind. Die Gruppen, die durch elliptische Kurven gegeben sind, haben sich in der Praxis dann als vorteilhaft herausgestellt.

Wenn wir Teilmengen von $\mathbb{Z}$ auch praktisch untersuchen möchten, wird die Frage wichtig, wie man ganze Zahlen auf geschickte/kompakte Art darstellen kann. Dafür benutzen wir im Alltag das Dezimalsystem, für Rechenmaschinen ist auch das Binär- und das Hexadezimalsystem nützlich. Dafür werden die Ziffern $0,1,\dots,9$ bzw. $0,1$ bzw. $0,1,\dots,9,A,\dots,F$ verwendet. Allgemein erhalten wir die g-adische Darstellung von $n\in\mathbb{N}$ so:

8.) **Satz:** Sei $g\in\mathbb{N}$, $g\geq 2$ und $n\in\mathbb{N}$. Dann gibt es ein $k\in\mathbb{N}_0$ und $c_k,c_{k-1},\dots,c_0\in\{0,\dots,g-1\}$ (genannt "Ziffern"), so dass $n = c_k g^k + c_{k-1}g^{k-1} + \dots + c_0 = \sum_{i=0}^{k} c_i g^i$.
Fordern wir $c_k\neq 0$, ist k und die Folge $c_k,\dots,c_1,c_0$ eindeutig bestimmt.

9.) **Def.:** Die Ziffernfolge $c_k,c_{k-1},\dots,c_0$ heißt g-adische Darstellung von n.
Die Zahl a_k heißt Leitziffer, die Zahl c_0 die Endziffer.
Die Zahl $k+1$ heißt Stellenzahl bzw. Länge der g-adischen Darstellung.
Die Zahl g heißt auch Basis der Darstellung.
Eine m-Bit-Zahl ist eine Zahl $n\in\mathbb{N}$ der Länge $\leq m$ zur Basis 2.

10.) **Bem.:** Wir können jede natürliche (und dann auch jede ganze) Zahl n also eind. schreiben als Linearkombination endlich vieler Potenzen von g.

11.) **Bsp.:** $163_{(10)} = 1\cdot 10^2 + 6\cdot 10^1 + 3\cdot 10^0$,

$43_{(10)} = 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 101011_{(2)}$

$= 2\cdot 16^1 + 11\cdot 16^0 = 2B_{(16)}$

Die bekannten schriftlichen Additions- und Multiplikationsrechnungen, die unter Beachtung von Überträgen ziffernweise geschehen, können in jeder Basis ausgeführt werden. Es gibt weiter für die Multiplikation großer Zahlen (d.h. mit großer Stellenzahl bis $\gtrsim 2\cdot 10^{10}$) schnelle Algorithmen, die wir hier aber nicht näher behandeln möchten; etwa mit der schnellen Fouriertransformation (FFT) nach Schönhage/Strassen.

Bew. von Satz 8): ($\Leftrightarrow k\log g \le \log n < (k+1)\log g$)

Existenz: Sei $k \in \mathbb{N}_0$ so, dass $g^k \le n < g^{k+1}$ gilt, d.h. wir setzen $k := \left\lfloor \frac{\log n}{\log g} \right\rfloor$, zeigen Ex. durch vollst. Ind. nach k:

Gaußklammer: $\lfloor x \rfloor := \max\{k \in \mathbb{Z};\ k \le x\}$

$k=0$: Setze $c_0 := n$.

$k \to k+1$: Sei $g^{k+1} \le n < g^{k+2}$ und setze $n' := n - \left\lfloor \frac{n}{g^{k+1}} \right\rfloor g^{k+1}$.
Es folgt $0 \le n' < g^{k+1}$, d.h. auf n' ist die Induktionsvor. anwendbar. Nach dieser hat n' die g-ad. Darst. $n' = \sum_{i=0}^{k} c_i g^i$.
Wegen $1 \le \frac{n}{g^{k+1}} < g$ ist $1 \le \left\lfloor \frac{n}{g^{k+1}} \right\rfloor < g$, also nimm $c_{k+1} := \left\lfloor \frac{n}{g^{k+1}} \right\rfloor$, erhalten so die g-ad. Darst. $n = c_{k+1} g^{k+1} + n' = \sum_{i=0}^{k+1} c_i g^i$.

Eindeutigkeit: Sind $\sum_{i=0}^{k} a_i g^i = n = \sum_{i=0}^{r} b_i g^i$ zwei Darstellungen von $n \in \mathbb{N}$, ist $r > k$, sei $a_{k+1} = \ldots = a_r := 0$, sonst sei $b_{r+1} = \ldots = b_k := 0$ falls $r < k$.
Dann sei $\ell := \max\{i \in \mathbb{N}_0;\ i \le \max\{k,r\},\ a_i \ne b_i\}$ die größte Stelle, an der sich die Darstellungen unterscheiden. Es folgt:

$$0 = \sum_{i=0}^{\max\{r,k\}} (a_i - b_i) g^i = \sum_{i=0}^{\ell} (a_i - b_i) g^i \Rightarrow |b_\ell - a_\ell|\, g^\ell = \left| \sum_{i=0}^{\ell-1} (a_i - b_i) g^i \right|$$

($a_i - b_i = 0$ für $i > \ell$; $|b_\ell - a_\ell| \ge 1$)

$$\Rightarrow\ g^\ell \le \sum_{i=0}^{\ell-1} |a_i - b_i| g^i \le \sum_{i=0}^{\ell-1} (g-1) g^i = (g-1)\frac{g^\ell - 1}{g-1} = g^\ell - 1,\ \lightning$$

(Δ-ungl.; geom. Σ)

□

Der Beweis von Satz 8) zeigt, dass die Länge von n gleich $\left\lfloor \frac{\log n}{\log g} \right\rfloor + 1$ ist, soviele Ziffern müssen zum Hinschreiben/Eintippen von n angegeben werden. Bei verschiedenen Basen ändert sich hier nur der Faktor $\frac{1}{\log g}$ vor $\log n$. Deswegen sagt man, die Länge sei $O(\log n)$ und meint damit die Aussage $\exists C > 0 : k+1 \le C \cdot \log n$. "Landau-Symbolik" bzw. "Groß-OH-Notation"

Entscheidend für das Studium von $\mathbb{Z}$ ist der Grundbegriff der Teilbarkeit:

12) **Def.:** Für $a, b \in \mathbb{Z}$ ist a Teiler von b bzw. a teilt b, in Zeichen: $a \mid b$, falls $\exists\, c \in \mathbb{Z} : ac = b$. Ist a kein Teiler von b, schreibt man $a \nmid b$.

13) **Bsp.:** $3 \mid 12$, $4 \mid 0$, $0 \mid 0$, $7 \nmid 12$, $0 \nmid 4$. Es kann 0 nur die 0 teilen.

14) **Def.:** Eine natürliche Zahl $p \in \mathbb{N}$ heißt **Primzahl** (PZ, prim), wenn sie genau zwei Teiler in $\mathbb{N}$ besitzt (nämlich 1 und p, $1 \neq p$).
Eine nat. Zahl $n > 1$ heißt **zusammengesetzt**, falls n keine PZ ist.

Primzahlen sind die "Bausteine" der natürlichen Zahlen:

15) **Satz von der eindeutigen Primfaktorzerlegung (PFZ) bzw. Hauptsatz der (elementaren) Arithmetik:**

Jede natürliche Zahl $n > 1$ besitzt **genau eine** Darstellung

$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} = \prod_{i=1}^{r} p_i^{e_i}$$

mit $r \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_r$, mit $e_1, \ldots, e_r \in \mathbb{N}$ und $p_1 < p_2 < \ldots < p_r$.
Diese heißt die **Primfaktorzerlegung** (PFZ) von n.

16) **Bem.:** Lässt man die letzte Bedingung weg, ist die Darstellung eindeutig bis auf die Reihenfolge der Primpotenzen. Die Zahl e_i ist dabei die **Vielfachheit** (auch **Exponent** genannt), mit der p_i als Faktor in n auftritt, d.h. $p_i^{e_i} \mid n$, aber $p_i^{e_i+1} \nmid n$. Dafür gibt es das Symbol $p^{e_i} \| n$, und die PFZ lässt sich kompakt auch schreiben als $n = \prod_p p^{e(p)}$, wobei $e(p) := e$ mit $p^e \| n$ falls $p \mid n$, und $e(p) := 0$ falls $p \nmid n$.
Weiter ist $\omega(n) := r$ die Anzahl der versch. Primteiler von n.

Beweis des Satzes 15): Existenz: Ist n prim, ist nichts z.z., und ist n nicht prim, gibt es $k, l \in \mathbb{N} \setminus \{1\}$ mit $n = k \cdot l$.
Da $\min\{k, l\} > 1$, folgt $\max\{k, l\} < n$. Nach Induktionsvor. sind also k, l Produkte von Potenzen von PZen also auch $n = k \cdot l$.
Die Eindeutigkeit zeigen wir erst später als Anwendung von Lemma 21). □

Bsp.: die PFZ von 360 ist $360 = 2^3 \cdot 3^2 \cdot 5$, d.h. $e(2) = 3$, $e(3) = 2$, $e(5) = 1$, und sonst $e(p) = 0$ für $p \notin \{2, 3, 5\}$.

Die Eindeutigkeit der PFZ zeigt, dass auch die PFZ eine Möglichkeit zur Darstellung natürlicher Zahlen ist. Diese ist jedoch unpraktisch, weil das folgende Problem i.a. schwer zu lösen ist, worauf einige kryptographische Verfahren (insb. RSA) beruhen:

17) **Faktorisierungsproblem:** Zu einer natürlichen zusammengesetzten Zahl $n > 1$ bestimme man einen nichttrivialen Teiler t mit $1 < t < n$.

Klar: Ist das Faktorisierungsproblem rechnerisch leicht zu machen, kann auch (durch Iteration) die PFZ von n leicht bestimmt werden.
In der Praxis, wenn n nicht gerade schon von einer spezieller Form ist, können Teiler großer Zahlen n jedoch nur sehr schwer aufgefunden werden.

▸ Das derzeit schnellste algorithmische Verfahren zur Faktorisierung (auf einem klassischen Computer) ist das Zahlkörpersieb mit einer Laufzeit von nur $O(\exp(C(\log n)^{1/3}(\log\log n)^{2/3}))$, d.h. es handelt sich um ein sogenanntes subexponentiell schnelles Verfahren, weil

$$(\log n)^B \ll \exp(C(\log n)^{1/3}(\log\log n)^{2/3}) \ll \exp(D\log n) = n^D.$$

($(\log n)^B$: polynomiell in $\log n$; mittlerer Term: irgendwo dazwischen...; $\exp(D\log n)$: exponentiell in $\log n$; [Inputgröße: $O(\log n)$])

▸ P. Shor entdeckte um 1994, dass das Faktorisierungsproblem auf einem Quantencomputer mit einer Laufzeit von (meist) nur $O((\log n)^3)$ sehr (d.h. polynomiell) schnell gelöst werden kann, was die Sicherheit gängiger Kryptoverfahren wie RSA untergräbt. Allerdings ist die Konstruktion solcher Quantencomputer (physikalisch) extrem schwierig, diverse Forschergruppen arbeiten daran. Am 2.1.2014 meldete die Washington Post unter Berufung auf Dokumenten von E. Snowden, dass die NSA an der Entwicklung eines kryptologisch nützlichen Quantencomputers arbeitet, vgl. wikipedia "Quantencomputer".

Im folgenden besprechen wir noch den ggT zweier natürlicher Zahlen, der sich in vielerlei Hinsicht als wichtig und nützlich erweist:

18.) **Def:** Seien $a, b \in \mathbb{Z}$. Der ggT von a und b (größter gemeinsamer Teiler) in $\mathbb{N}$ ist die Zahl $d := \max\{t \in \mathbb{N}: t|a \wedge t|b\}$. Notation: $ggT(a,b) := d$.
Ist $ggT(a,b)=1$, heißen a und b teilerfremd. Haben wir für a und b die PFZen $a = \prod_p p^{e(p)}$ und $b = \prod_p p^{f(p)}$ vorliegen, kann ihr ggt leicht bestimmt werden als $ggT(a,b) = \prod_p p^{\min(e(p),f(p))}$, z.B. $ggT(2^3 \cdot 3^6 \cdot 5^4, 2^4 \cdot 3^5) = 2^3 \cdot 3^5$.
Wegen dem Faktorisierungsproblem kann dies aber so nicht praktisch umgesetzt werden. Stattdessen benutzt man den (polynomiell) schnellen euklidischen Algorithmus. [Dass dieser so schnell ist, wird eine (ü)-Aufgabe]

19.) **Satz** (Teilen mit Rest): Zu $a \in \mathbb{Z}, b \in \mathbb{N}$ ex. eind. $q, r \in \mathbb{Z}$, $0 \le r < b : a = qb + r$, nämlich $q = \lfloor \frac{a}{b} \rfloor = \max\{m \in \mathbb{Z}: m \le \frac{a}{b}\}$ und $r = a - qb$. Dabei heißt r der kleinste nichtnegative Rest. Statt $0 \le r < b$ kann auch $r \in \mathbb{Z}$, $|r| < \frac{b}{2}$, erfüllt werden; r heißt dann der absolut kleinste Rest (bei Division durch b).
L.J: Gaußklammer
Bew.: ✓ Bsp.: $20 = 7 \cdot 2 + 6 = 7 \cdot 3 + (-1)$
(6: kl. nn. Rest; −1: abs. kl. Rest)

20.) **Satz** (vom euklidischen Algorithmus): Seien $a, b \in \mathbb{N}$.
Durch fortgesetztes Teilen mit Rest erhalten wir als letzten Rest $\neq 0$ den $ggT(a,b)$, sowie $x, y \in \mathbb{Z}$ mit $ggT(a,b) = xa + yb$ laut Schema.

Beschreibung des Rechenverfahrens: (a, b)
Rechnen sukzessive: $r_{-1} := a$, $r_0 := b$, $r_{-1} = q_0 r_0 + r_1$, $r_0 = q_1 r_1 + r_2$, $r_1 = q_2 r_2 + r_3$, ...
Letzte Division: $r_{n-1} = q_n r_n$
→ Das Verfahren wird fortgeführt, bis erstmals ein Rest $r_{n+1} = 0$ auftritt, was wegen $r_0 > r_1 > r_2 > \dots$ nach höchstens $b+1$ vielen Schritten der Fall sein wird. Sind die Quotienten $q_0, \dots, q_n$ bekannt, können mit den Rekursionen $c_{-2} = 0$, $c_{-1} = 1$, und $c_k = q_k c_{k-1} + c_{k-2}$, $k = 0, 1, 2, \dots, n$, sowie $d_{-2} = 1$, $d_{-1} = 0$, sowie $d_k = q_k d_{k-1} + d_{k-2}$, $k = 0, 1, 2, \dots, n$, die Bézout-Elemente als $x = (-1)^{n-1} d_{n-1}$ und $y = (-1)^n c_{n-1}$ berechnet werden:

Schematisch:

q_k			q_0	q_1	q_2	...	q_{n-1}	q_n
c_k	0	1 →	q_0	c_1	c_2	...	$c_{n-1} \rightsquigarrow \pm y$	$a/ggT(a,b)$
d_k	1	0	1	d_1	d_2	...	$d_{n-1} \rightsquigarrow \pm x$	$b/ggT(a,b)$

Bsp.: $a = 360$, $b = 84 \rightsquigarrow 360 = 4 \cdot 84 + 24$, $84 = 3 \cdot 24 + 12$, $24 = 2 \cdot 12 + 0$ (ggT = 12)

q_k			4	3	2
c_k	0	1	4	13	$30 = \frac{360}{12}$
d_k	1	0	1	3	$7 = \frac{84}{12}$

$\rightsquigarrow 13 \cdot 84 - 3 \cdot 360 = 12$ (13 = y, 3 = x)

Wir behaupten also:

(1) Es ist $ggT(a,b) = r_m$.

(2) $ggT(a,b) = \underbrace{(-1)^{m-1} d_{m-1}}_{x}\, a + \underbrace{(-1)^m c_{m-1}}_{y}\, b$.

Bew.: Zu (1):

Da $r_m \mid r_{m-1}, r_m \mid r_{m-2}, \dots, r_m \mid r_0 = b, r_m \mid r_1 = a$, ist r_m Teiler von a und b ("Teilen mit Rest von unten nach oben")

Ist d irgendein Teiler ≥ 1 von a und b, folgt $d \mid r_1 = a - q_0 b \Rightarrow d \mid r_2 = r_0 - q_1 r_1 \Rightarrow d \mid r_3 = \dots$, also auch r_m, so dass $d \leq r_m$ folgt ("Teilen mit Rest von oben nach unten"). Somit ist $r_m = ggT(a,b)$.

Zu (2): Induktiv kann $c_{k-1} d_k - c_k d_{k-1} = (-1)^k$ gezeigt werden.

Daher gen. z.z.: $c_n = \frac{a}{ggT(a,b)}$, $d_n = \frac{b}{ggT(a,b)}$. [Bew.: Mit den $\frac{c_k}{d_k}$ wird die Kettenbruchentwicklung von $\frac{a}{b}$ berechnet und diese bricht bei $\frac{c_n}{d_n} = \frac{a}{b}$ ab. (ohne Bew.)

Einzelheiten → vgl. Lesestoff-Skript

Da beider KBE alle Brüche $\frac{c_k}{d_k}$ gekürzt sind wegen $c_{k-1} d_k - c_k d_{k-1} = (-1)^k$, folgt dies.] □

konstruktiv!

Der Satz 20.) vom euklidischen Algorithmus sichert uns ↓ also die Existenz ganzer Zahlen $x, y \in \mathbb{Z}$ mit $ggT(a,b) = xa + yb$. Die Zahlen x und y heißen auch Bézout-Elemente von a und b. Deren Existenz ist auch in der Theorie immer wieder wichtig, z.B. hierfür:

Bem.: Eigenschaft des ggT: $d = ggT(a,b)$, $c \mid a \wedge c \mid b \Rightarrow c \mid d$, denn $c \mid xa + yb = d$, $x, y \in \mathbb{Z}$.

21.) Lemma: $a, b, c \in \mathbb{Z}$, nicht $b = c = 0 \Rightarrow$ ($c \mid ab$ und $ggT(b,c) = 1 \Rightarrow c \mid a$)

Bew.: Vor. und $c \mid ac \overset{\text{Bem.}}{\Rightarrow} c \mid ggT(ab, ac) \overset{\otimes}{=} |a| \cdot ggT(b,c) = |a|$, also: $c \mid a$.

Noch zu ⊗: Nach Satz 20.) ex. $x, y \in \mathbb{Z}$ mit $ggT(b,c) = xb + yc$.

Haben: $|a| \cdot ggT(b,c)$ teilt $|a|b$ und $|a|c$, also auch ba und ca, d.h. die r.S. in ⊗ ist ein gem. Teiler von ba und ca. Ist t irgendein solcher, so teilt t auch $\operatorname{sign}(a)(xba + yca) = xb|a| + yc|a| = |a|(xb + yc) = |a|\, ggT(b,c)$. Es folgt ⊗. □

Bew. der Eindeutigkeit von Satz 15.):

Eindeutigkeit: Sei $n > 1$ minimal mit zwei versch. Zerlegungen $n = \prod_{i=1}^{r} p_i^{e_i} = \prod_{i=1}^{s} q_i^{f_i}$ ⊠ die p_i, q_i prim und angeordnet. Da $p_1 \neq q_i$ für alle i: gilt [sonst hätte $\frac{n}{p_1} < n$ zwei versch. Zerl.], ist $ggT(p_1, q_i) = 1$, und mit ⊠ folgt $p_1 \mid q_1^{f_1 - 1} \cdot \prod_{i=2}^{s} q_i^{f_i}$ aus Lemma 21.). Die Fortsetzung des Verfahrens zeigt schließlich $p_1 \mid q_s$, was wegen $ggT(p_1, q_s) = 1$ ein ↯ ist. □

(Beachten Sie: zum Bew. wurde nie die (eind.) PFZ von Zahlen benutzt!) □