1 Primzerlegung

1.1 Faszination Primzahlen: Primzahlsatz (o.Bew.), gelöste und ungelöste Probleme über Primzahlen

Satz 1.1 (Euklid, ca. 300 v. Chr.)

$$\#\mathbb{P} = \infty$$

Bemerkung: Analysis:

$$\sum_{n\in\mathbb{N}} \frac{1}{n} = \infty$$
$$\sum_{n\in\mathbb{N}} \frac{1}{n^2} < \infty$$

Euler:

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty$$

Definition
$p \in \mathbb{P}$ heiße Zwillingsprimzahl $\iff p, p+2 \in \mathbb{P}$

$\{p, p+2\}$ heißt Primzahlzwilling

Frage: Gibt es unendlich viele Primzahlzwillinge? Kein Mensch hat eine Idee, wie das zu zeigen ist.

Satz 1.2 (Primzahlzwillingsatz von Viggo Brun, ca. 1915)

$$\sum_{p \text{ Zwillingsprimzahl}} \left(\frac{1}{p} + \frac{1}{p+2}\right) < \infty$$

Pierre de Fermat (1601 – 1665) schreibt auf den Rand seines Exemplars von Arithmetica des Diophant: „Die Gleichung $x^n + y^n = z^n$ (mit $n \in \mathbb{N}$, $n > 2$) hat keine Lösung mit $x, y, z \in \mathbb{N}_+$“.
Heute: Fermat hat recht. (Wiles 1995/96)

Fermat schrieb auch: Die Zahlen $F_n = 2^{(2^n)} + 1$ sind prim. Die Aussage ist ok für $n = 0, 1, 2, 3, 4$.
Euler konnte zeigen, dass $F_5 = 4294967297 = 641 \cdot 6700417$. Noch 2000 ist unbekannt, ob F_{24} prim ist.

Möglichkeiten:

(1) Kein F_n mit $n > 24$ ist prim.

(2) Nur endlich viele F_n sind prim.

(3) $\#\{F_n | F_n \in \mathbb{P}\} = \infty$

(4) $\#\{F_n | F_n \notin \mathbb{P}\} = \infty$

Niemand weiß oder vermutet, was richtig ist, keine Beweisideen!

Definition
$M_p = 2^p - 1$ heißt p-te Mersenne-Zahl

Satz 1.3
M_p ist höchsten dann prim, wenn $p \in \mathbb{P}$

Beweis
Übungsaufgabe ∎

Die größte bekannte Primzahl ist seit längerem eine Mersenne-Primzahl, da es gute Tests gibt, z.B. Lucas/Lehmer, verbessert von Grandall. Heute: $M_p \in \mathbb{P}$ für $p = 3021327$, $M_p > 10^{2000000}$.

Eine weitere Frage an Primzahlen ist die nach der Verteilung von $\mathbb{P}$ in $\mathbb{N}$. Bei dieser Frage spielt die Analysis eine Rolle.

Satz 1.4 (Elementarer Primzahlsatz)
Sei $\Pi(x) = \#\{p \in \mathbb{P} | p \leq x\}$ $(x \in \mathbb{R})$. Dann gilt:

$$\Pi(x) \sim \frac{x}{\log x} \text{ (fast asymptotisch gleich)}$$

Der Satz wurde 1792 von Gauß vermutete und 1896 von Hadamard und von de la Vaille-Poussin nach Vorarbeiten von Riemann bewiesen

Folgerung 1.5
Sei p_n die n-te Primzahl der Größe nach $(p_1 = 2, p_2 = 3, p_3 = 5, \ldots)$. Dann gilt:

$$p_n \sim n \cdot \log n \quad (n \to \infty)$$

Beweis
$p_n = x \implies n = \Pi(x)$

$$\begin{aligned}
\lim_{n\to\infty} \frac{n \cdot \log n}{p_n} &= \lim_{n\to\infty} \frac{\Pi(x) \log \Pi(x)}{x} \\
&= \lim_{n\to\infty} \frac{\Pi(x)}{x/\log x} \cdot \frac{x}{\log x} \cdot \frac{\log \Pi(x)}{x} \\
&= \lim_{n\to\infty} \frac{\log \Pi(x)}{\log x} \\
&= \lim_{n\to\infty} \frac{1}{\log x} \cdot \log \frac{\Pi(x)}{x/\log x} x/\log x \\
&= \lim_{n\to\infty} \frac{1}{\log x} \left(\log \frac{\Pi(x)}{x/\log x} + (\log x - \log\log x) \right) \\
&= 1 - \lim_{x\to\infty} \frac{\log(\log x)}{\log x} \\
&= 1 - \lim_{t\to\infty} \frac{\log t}{t} \\
&= 1 - \lim_{n\to\infty} \frac{n}{e^n} = 1
\end{aligned}$$

■

Folgerung 1.6
$\forall \varepsilon > 0\ \exists N \in \mathbb{N}\ \forall x \geq N\ \exists p \in \mathbb{P}$:

$$x \leq p \leq x(1+\varepsilon)$$

Riemann (1826–66): „Über die Anzahl der Primzahlen unter einer gegebenen Größe“ stellt Zusammenhang mit Riemanns ζ-Funktion her.

$$\zeta(s) = \sum_{n\in\mathbb{N}_+} \frac{1}{n^s}, s \in \mathbb{C}$$

$\zeta(s)$ konvergiert für $\operatorname{Re} s > 1$ und hat eindeutige Fortsetzung zum analytischer Funktion $\mathbb{C}\setminus 1 \to \mathbb{C}$ mit Pol in $s = 1$. Man kann zeigen: Primzahlsatz $\iff$ ζ hat keine Nullstelle mit $\operatorname{Re} \geq 1$.

Vermutung: Alle nichtreellen Nullstellen von ζ liegen auf $\frac{1}{2} + i\mathbb{R}$. Gauß vermutet: Besser als $x/\log x$ approximiert

$$\operatorname{li}(x) = \int_2^x \frac{du}{\log u} \quad \text{(Integrallogarithmus)}.$$

Man will möglichst gute Abschätzung des Restglieds $R(x) = |\Pi(x) - \operatorname{li}(x)|$.

Fakt: Je größer die nullstellenfreien Gebiete von ζ, desto bessere Restgliedabschätzung möglich. Demnach: Beste Restgliedabschätzung möglich, wenn Riemanns Vermutung stimmt.

$$R(x) \leq \text{Const} \cdot x^{\frac{1}{2}} \log x$$

Fakt 2: Von der Qualität der Restgliedabschätzung hängen in der Informatik viele Aussagen über die theoretische Effektivität von numerischen Algorithmen ab.

1.2 Elementare Teilbarkeitslehre in integren Ringen

In dieser Vorlesung gilt die Vereinbarung, dass ein Ring definitionsgemäß genau ein Einselement 1_R besitzt.

Definition
Ein Ring R heißt *integer*, wenn gilt:

(1) R ist kommutativ.

(2) $\forall a, b \in R: \ ab = 0 \iff a = 0 \vee b = 0.$

Beispiel
Jeder Unterring eines Körpers ist integer.

Definition
Die Menge

$$R^\times := \{a \in R | \ \exists x \in R: \ ax = 1 = xa\}$$

heißt *Einheitengruppe* $R^\times$ des (allgemeinen) Ringes R.
Leicht zu sehen ist, dass $R^\times$ eine Gruppe ist, x ist das eindeutig bestimmte Inverse a^{-1} von a.

Beispiel
$\mathbb{Z}^\times = \{\pm 1\}$ (klar!)
$\mathbb{Z}^{n\times n}$ ist der Ring der ganzzahligen $n \times n$-Matrizen, $GL(\mathbb{Z}) = (\mathbb{Z}^{n\times n})^\times$. Beispielsweise für $n = 2$:

$$A = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}, \ A^{-1} = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}, \ A\,A^{-1} = I = A^{-1}\,A \Rightarrow A \in GL_2(\mathbb{Z}).$$

$R = K[X]$ ist der Ring der Polynome in X über dem Körper K. $R^\times = \{\alpha \in K^\times = K\backslash\{0\}\}$ (Konstante, von 0 verschiedene Polynome)
$\mathbb{Z}, K[X]$ sind integere Ringe.

Ab jetzt sei R ein integerer Ring, $a, b, c, d, x, y, u, v, w \in R$.

Problem: Gleichung $ax = b$ mit der Variablen x. Beispielsweise ist $3x = 5$ in $R = \mathbb{Z}$ nicht lösbar, $3x = 6$ hingegen schon.

Definition

$$a|b \iff \exists x \in R: \ ax = b$$

Sprechweise: a teilt b, b ist Vielfaches von a, a ist Teiler von b.

$\neg a|b \iff a \nmid b$ (a teilt nicht b).

Beispiel
$R = \mathbb{Z}$: $3 \nmid 5, \ 3|0, \ \pm 3, \ \pm 6 \ldots$
$R = K[X]$: $(X-1)|(X^2-1)$.
In jedem R: $\forall a \in R: 1|a$ (denn $a = a \cdot 1$) $\wedge$ $a|0$ (denn $0 = 0 \cdot a$).

Satz 1.7 (Elementare Teilbarkeitseigenschaften)

(1) | ist mit $\cdot$ verträglich:
$a|b \ \wedge \ c|d \Rightarrow ac|bd$.

(2) | ist mit Linearkombinationen verträglich:
$a|b \ \wedge \ a|c \Rightarrow \ \forall x, y \in R: \ a|xb + yc$.

(3) | ist eine transitive und reflexive Relation und für $a \neq 0$ gilt:
$a|b \ \wedge \ b|a \iff \exists e \in R^\times: \ a = eb$.

Beweis
Treppenbeweis © Dr. Rehm. ∎

Bemerkung: (2) hat einen häufigen Spezialfall: $a|b \ \wedge \ a|c \Rightarrow a|b \pm c$.
Anwendungsbeispiel: $a|b^2 \ \wedge \ a|b^2 + 1 \Rightarrow a|\underbrace{b^2 + 1 - b^2}_{=1}$.
Folgerung: $e \in R^\times: \ a|b \iff ea|b \iff a|eb$.
Grund: $b = xa = (xe^{-1})ea$.
Merke: Einheitsfaktoren ändern Teilbarkeit nicht!
Folge 2: R ist disjunkte Vereinigung aller Mengen $R^\times a = \{ea|e \in R^\times\}$.
Grund: $u \in R^\times a \cap R^\times b \iff u|a \ \wedge \ a|u \ \wedge \ u|b \ \wedge b|u$, also $R^\times a = R^\times u (= R^\times b$, $eu \in R^\times a \Rightarrow R^\times u \subset R^\times a$, genauso zeigt man $R^\times a \subset R^\times u$.

Definition (Normierung)
Auswahl je eines festen a_{nor} in $R^\times a$. Man wählt immer $e_{nor} = 1, \ 0_{nor} = 0$.
Standard-Normierung: $R = \mathbb{Z}, \ R^\times a = \{\pm a\}, \ a_{nor} = \max\{R^\times a\} = |a|$.
$R = K[X], \ 0 \neq f = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$ mit $\alpha_n \neq 0$. Dann ist $f_{nor} = \frac{1}{\alpha_n} f$.

Klar ist: Jedes $a \in R$ hat die trivialen Teiler $e \in R^\times$ und $ea, e \in R^\times$. Nichttriviale Teiler heißen auch echte Teiler.

Beispiel
$R = \mathbb{Z}$, triviale Teiler von 6 sind $\pm 1, \ \pm 6$. Echte Teiler sind $\pm 2, \ \pm 3$.

Definition

(1) $a \in R$ heißt unzerlegbar oder irreduzibel, falls $a \neq 0, \ a \notin R^\times$ und a hat nur triviale Teiler.

(2) $R = \mathbb{Z}$. $p \in \mathbb{Z}$ heißt Primzahl $\iff$ p normiert und irreduzibel.

(3) $R = K[X]$. $f \in R$ heißt Primpolynom $\iff$ f irreduzibel.

Größter gemeinsamer Teiler und kleinstes Gemeinsames Vielfaches

Definition
d heißt ein größter gemeinsamer Teiler von $a_1, a_2, \ldots, a_n :\iff$

(1) $d|a_1 \ \wedge \ d|a_2 \ \wedge \ \cdots \ \wedge \ d|a_n$ (d ist gemeinsamer Teiler)

(2) $u|a_1 \ \wedge \ u|a_2 \ \wedge \ \cdots \ \wedge \ u|a_n \Rightarrow u|d$

Bemerkung: (1) Bei $R = \mathbb{Z}$ ist ein bezüglich $\leq$ größter gemeinsamer Teiler ein normierter ggT.

(2) Eindeutigkeit des ggT: Ist d ein ggT von $a_1, a_2, \ldots, a_n$, so ist auch d_{nor} ein ggT und d_{nor} ist durch $a_1, a_2, \ldots, a_n$ eindeutig bestimmt: $d = d_{nor} = \text{ggT}(a_1, a_2, \ldots, a_n)$
Grund: $e \in R^\times$ spielt bei Teilbarkeit keine Rolle, und $d_{nor} = ed$ für ein $e \in R^\times$. Sind d, d' ggTs von $a_1, a_2, \ldots, a_n \Rightarrow d|d' \ \wedge \ d'|d \iff d' = ed$, da normiert $\Rightarrow d = d'$.

Der kgV wird analog zum ggT unter Umkehrung aller Teilbarkeitsrelationen definiert:

Definition
k heißt ein kgV von $a_1, a_2, \ldots, a_n :\iff$

(1) $a_1|k \ \wedge \ a_2|k \ \wedge \ \cdots \ \wedge \ a_n|k$ (k ist gemeinsames Vielfaches)

(2) $a_1|u \ \wedge \ a_2|u \ \wedge \ \cdots \ \wedge \ a_n|u \Rightarrow k|u$

Die Eindeutigkeitsaussage des ggT gilt für den kgV ebenfalls.

Satz 1.8 (Euklids Primzahlsatz)
Für $R = \mathbb{Z}$ gilt:

$$\#\mathbb{P} = \infty$$

Beweis
Es seien $p_j, \ j = 1, 2, \ldots, n$ paarweise verschiedene Primzahlen. Betrachte $1 + \prod p_i > 0$.
Aussage: Ist $a \in \mathbb{N}, \ a > 1$, so ist $\min\{d \in \mathbb{N} : d|a\}$ eine Primzahl und das Minimum existiert wegen $a|a$. Benutzt, dass jede Teilmenge der natürlichen Zahlen eine kleinste Zahl enthält $\Rightarrow$ Behauptung, da ein echter Teiler kleiner wäre $\Rightarrow \exists p \in R : \ p|1 + \prod p_j$.
Wäre $p = p_j$ für ein $j \in \{1, 2, \ldots, n\}$, so $p|\prod p_j$. $p|\underbrace{1 + \prod p_j - 1(\prod p_j)}_{=1} \iff p|1 \Rightarrow p \in \mathbb{Z}^\times \Rightarrow$
Widerspruch. ∎

1.3 Primzerlegung in Euklidischen Ringen, Faktorielle Ringe

In diesem Abschnitt sei R integerer Ring, $a, b, c, d, \ldots \in R$.
Sprechweise: $a = qb + r$. Man sagt r ist der Rest bei Division von a durch b, q ist der Quotient (Division mit Rest).
Mathematischer Wunsch: Rest r soll im geeigneten Sinn kleiner sein als der Divisor b. Man benötigt dafür eine Größenfunktion $gr : \ R \mapsto \mathbb{N}$.

Definition
Ein Ring R, beziehungsweise ein Paar (R, gr) heißt euklidisch $:\iff$

(1) R ist integer

(2) Man hat Division mit Rest, das heißt:
$\forall a, b \in R, \ b \neq 0, \ \exists q, r \in R : a = qb + r$, wobei $r = 0$ oder $gr(r) < gr(b)$.

Es ist $(\mathbb{Z}, |\cdot|)$ ein euklidischer Ring.

Beweis
O.b.d.A: $b > 0$, da $|b| = gr(b) = gr(-b)$.

$q = \lfloor \frac{a}{b} \rfloor$ ist geeignet: $0 \leq \frac{a}{b} - q < 1 | \cdot b \Rightarrow 0 \leq a - qb = r < b \Rightarrow gr(r) = |r| = r < b = |b| = gr(b)$ ■

Viele Porgrammiersprachen, etwa MAPLE, bieten einen modulo-Operator:
`r := (a mod b)` $= a - \lfloor \frac{a}{|b|} \rfloor$.

Im $K[X]$ ist die Division mit Rest möglich bezüglich $gr(f) := \operatorname{grad} f = n$, $(f \neq 0)$.

Der Ring $R = \mathbb{Z} + \mathbb{Z}i \subset \mathbb{C}$, also $R = \{x + iy | x, y \in \mathbb{Z}\}$ heißt „Ring der ganzen Gaußschen Zahlen". R ist euklidisch mit $gr(x, iy) = |x + iy| = \sqrt{x^2 + y^2}$. Die Idee für die Division mit Rest ist: Suche einen Gitterpunkt nahe $\frac{a}{b}$. (siehe Übung)

Lemma 1.9
R integer, $a = qb + r$, $a, b, q, r \in R$. Dann gilt

$$\operatorname{ggT}(a, b) = \operatorname{ggT}(b, r)\,,$$

und falls eine Seite existiert, so auch die andere.

Beweis
Sind $u, v \in R$, so kann Existenz und $\operatorname{ggT}(u, v)$ abgelesen werden an

$$T(u, v) = \{d \in R \big| d|u \wedge d|v\}\,,$$

der Menge der gemeinsamen Teiler. Es ist aber $T(a, b) = T(b, r)$:
„$\subseteq$": $d|a \wedge d|b \implies d|r$ (Linearkombination)
„$\supseteq$": $d|r \wedge d|b \implies d|a$ (Linearkombination) ■

Euklids glänzende Idee ist nun: Bei der Division mit Rest verkleinert der Übergang von (a, b) zu (b, r) das Problem. Sein Algorithmus ist wie folgt:

```
ggT := proc(a,b);          # Prozedur, die ggT = ggT(a,b)
aus $a$,$b$ berechnet if b = 0
  then normiere(a)         # es ist immer ggT(a,0) = a_nor
  else ggT(b, a mod b)     # terminiert wegen gr(a mod b) < gr(b)
fi
```

Idee: r ist Linearkombination von a und a, b. Die Hoffnung dabei ist: Auch $d := \operatorname{ggT}(a, b)$ lässt sich linear kombinieren.

Satz 1.10 (Satz der Linearkombination des ggT)
Sei R ein euklidischer Ring. Dann existiert $d = \operatorname{ggT}(a, b)$ für alle $a, b \in R$ und ist als R-Linearkombination von a, b, darstellbar:

$$\exists x, y \in R : d = \operatorname{ggT}(a, b) = xa + yb$$

Beweis

I Falls $b = 0$ („Induktionsanfang“) gilt $d = a_{\text{nor}} = e \cdot a + 0 \cdot b$ mit geeignetem $e \in R^\times$

II Falls $b \neq 0$: Division mit Rest $a = qb + r$
Falls $r = 0$ ist $d = b_{\text{nor}}$, fertig!
Falls $r \neq 0$, so gilt $\text{ggT}(a, b) = \text{ggT}(b, r) = d$ und $gr(r) < gr(b)$

Induktionshypothese: $\exists x_0, y_0 \in R$: $d = x_0 b + y_0 r = x_0 b + (a - qb)y_0 = y_0 a + (x_0 - q y_0)b = xa + yb$
Induktionsschritt geleistet. ∎

Die Idee ist, dass ein Ring *faktoriell* heißt, wenn man in ihm eine eindeutige Primzerlegung, wie aus $\mathbb{Z}$ bekannt, hat. Ein Ziel der Vorlesung ist die Feststellung, dass euklidische Ringe faktoriell sind (Euler-Faktoriell-Satz).

Definition
Ein Ring R heißt faktoriell (älter: „ZPE-Ring“) wenn gilt:

(i) R ist integer

(ii) Es gibt eine Menge $P \subseteq R$, bezüglich der jedes $a \in R$ mit $a \neq 0$ eine „eindeutige Primzerlegung“ hat, also:

$\exists e(a) \in \mathbb{R}^\times \; \exists v_p(a) \in \mathbb{N}$, mit nur endlich vielen $v_p(a) \neq 0$ mit

$$a = e(a) \cdot \prod_{p \in P} p^{v_p(a)} \text{ „Primzerlegung von } a\text{“}$$

Eindeutigkeit heißt: Durch a sind $e(a)$ und alle $v_p(a)$ eindeutig bestimmt.

Der Fall $R = \mathbb{Z}$ ist aus der Schule bekannt, und wird nicht bewiesen. Ein Beispiel ist $-100 = -1 \cdot 2^2 \cdot 5^2$, also $e(-100) = -1$, $v_2(-100) = v_5(-100) = 2$ und $\forall p \in P, p \neq 2, p \neq 5 : v_p(-100) = 0$

Im Fall $R = K$, wobei K ein Körper ist, gilt $R^\times = \mathbb{K} \setminus \{0\}$ und $P = \emptyset$.

Ist R faktoriell, so ist die Standardnormierung

$$a_{\text{nor}} = \prod_{p \in P} p^{v_p(a)} \, .$$

Bemerkung: P besteht aus unzerlegbaren Elementen. Hätte man nämlich $p = uv$ mit echten Teilern u, v, so gilt $u, v \notin R^\times$, also $\forall p_1, p_2 \in P$: $v_{p_1} > 0, v_{p_2} > 0$. Nun haben wir zwei Primzerlegungen, da $v_p(p) = 1$, $\forall q \in P, q \neq p, v_q(p) = 0$ und damit $p = 1 \cdot p^1 = 1 \cdot p_1^1 \cdot p_2^1$

Ein Zweck der Primfaktorzelegung ist, dass die Multiplikation in R auf die $R^\times$ und die Addition in $\mathbb{N}$ zurückgeführt werden kann. Denn mit $a = e(a) \cdot \prod_{p \in P} p^{v_p(a)}$, $b = e(b) \cdot \prod_{p \in P} p^{v_p(b)}$ gilt:

$$\begin{aligned} ab &= e(a) \cdot e(b) \cdot \prod_{p \in P} p^{v_p(a) + v_p(b)} \\ &= e(ab) \cdot \prod_{p \in P} p^{v_p(ab)} \end{aligned}$$

Aus der Eindeutigkeit folgt nun: $e(ab) = e(a) \cdot e(b)$ und $v_p(ab) = v_p(a) + v_p(b)$. $v_p(a)$ heißt „additiver p-Wert von a“. v_p heißt (additive) p-adische Bewertung von R.

Ein weiterer Zweck liegt in der Rückführung der Teilbarkeit auf $\leq$ in $\mathbb{N}$: Für $a, b \neq 0$ gilt

$$b|a \iff \forall p \in P : v_p(b) \leq v_p(a)$$

Begründung: $nb = a \implies v_p(b) \leq v_p(b) + \underbrace{v_p(n)}_{\geq 0} = v_p(a)$

Eine Folgerung davon ist, dass $\forall p \in P$ gilt: $v_p(\mathrm{ggT}(a,b)) = \min\{v_p(a), v_p(b)\}$ und allgemeiner: $v_p(\mathrm{ggT}(a_1, \ldots, a_n)) = \min\{v_p(a_1), \ldots, v_p(a_n)\}$. (Damit das auch bei $a = 0$ Sinn macht, kann man $v_p(0) = \infty$ definieren, was auch üblich ist.) Ebenso gilt: $\forall p \in P$: $v_p(\mathrm{kgV}(a,b)) = \max\{v_p(a), v_p(b)\}$.

Allerdings ist zur Bestimmung von $\mathrm{kgV}(a,b)$ folgener Algorithmus besser als der Weg über die Primfaktorzelegung:

(1) Berechne $\mathrm{ggT}(a,b)$ mit Euklids Algorithmus

(2) Verwende: Sind a, b normiert, so gilt:

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = ab$$

Begründung: $\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} = v_p(a) + v_p(b)$ und $ab = \prod_{p \in P} p^{v_p(a)+v_p(b)}$

Anwendungsbeispiel: Ist $m, n \in \mathbb{N}_+$, so gilt $\mathrm{ggT}(a^m, b^n) = 1 \iff \mathrm{ggT}(a,b) = 1$

Zusammenfassung: Für alle $a, b \in R$, $a, b \neq 0$ gilt:

- $v_p(ab) = v_p(a) + v_p(b)$
- $a \in R^\times \iff \forall p \in P : v_p(a) = 0$
- $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$
- $v_p(\mathrm{ggT}(a,b)) = \min\{v_p(a), v_p(b)\}$

Noch zu zeigen: $v_p(a+b) \geq \min(v_p(a), v_p(b))$.
O.B.d.A: $v_p(a) \leq v_p(b)$, also $\min(v_p(a), v_p(b)) = v_p(a)$. $a = p^{v_p(a)} \cdot a_0$, $b = p^{v_p(b)} b_0$ mit $a_0, b_0 \in \mathbb{R}$.
$a + b = p^{v_p(a)}(a_0 + p^{v_p(b)-v_p(a)} b_0) \Rightarrow p^{v_p(a)} | a+b \Rightarrow v_p(p^{v_p(a)}) = v_p(a) \leq v_p(a+b)$

Bemerkung: Ist R (integrer Rang) enthalten in einem Körper, so ist $K = \{\frac{a}{b} = x | a, b \in R, b \neq 0\}$ ein Körper.
Man kann v_p auf K ausdehnen: $v_p(x) = v_p(a) - v_p(b)$ $(x \neq 0)$ Ist R faktoriell, so hat man die „Primzerlegung“ von $x = \frac{a}{b}$:

$$x = e(x) \cdot \prod_{p \in P} p^{v_p(x)}$$

mit $e(x) \in R^\times, v_p(x) \in \mathbb{Z}$. Nur endlich viele $v_p(x)$ sind $\neq 0$.
$x \in R \Leftrightarrow v_p(x) \geq 0$ $(\forall p \in P)$. Die Rechenregeln 1-4 gelten auch auf K (siehe R [Beweis leicht]).

Beispiel
$v_7(\frac{7}{25}) = 1, v_5(\frac{7}{25}) = -2, v_p(\frac{7}{25}) = 0$ sonst

Lemma 1.11
Sei R euklidisch, dann gibt es eine „Größenfunktion“ $gr : R \to \mathbb{N}$ für die (zusätzlich) gilt:

- Ist $e \in R^\times, a \in R, a \neq 0 : gr(ea) = gr(a)$
- Ist b ein *echter* Teiler von $a \neq 0$, so ist $gr(b) < gr(a)$

Beweis
Idee: Ist gr die gegebene Größenfunktion, so erfüllt

$$gr^*(a) = \min\{gr(ea) | e \in R^\times\}$$

die beiden Punkte des Lemmas. (Beweis wird auf die Homepage gestellt!) ∎

Für $R = \mathbb{Z}$ und $R = K[X]$ sind beide ohnehin richtig.
(z.B. $\mathbb{Z}, gr(a) = |a|, b$ echter Teiler. $a = bu, u \in \mathbb{Z}^\times = \{\pm 1\} \Rightarrow |a| > 1 \Rightarrow gr(a) = |a| = |b||u|, gr(b) = |b| = \frac{|a|}{|u|} < |a| = gr(a)$. Ähnlich in $K[x]$)

Lemma 1.12
R sei euklidisch, $p \in R$ irreduzibel, $a, b \in R$. Dann gilt:

$$p|ab \implies p|a \text{ oder } p|b$$

Beweis
O.B.d.A.: p normiert, die normierten Teiler von p sind 1 und p.
Annahme: $p \nmid a \wedge p \nmid b$
Falls $p \nmid a \Rightarrow \mathrm{ggT}(p, a) = 1$
(anderenfalls $\mathrm{ggT}(p, a) = p$, damit $p|a$, Widerspruch!).
$p \nmid b \Rightarrow \mathrm{ggT}(p, b) = 1$.
Nach dem Linearkombinations-Satz:

$$\exists x_0, y_0, x_1, y_1 \in R : 1 = x_0 p + y_0 a = x_1 p + y_1 b$$
$$1 = 1 \cdot 1 = \underbrace{(...)}_{\in R} p + y_0 y_1 ab$$

$p|ab \Rightarrow p|1 \Rightarrow p \in R^\times$, also nicht irreduzibel, Widerspruch! ∎

Beweis
Des Euler-Faktoriell-Satzes: R euklidisch $\Rightarrow R$ faktoriell.
$P = \{p_{\mathrm{nor}} | p \text{ irreduzibel}\}$ (z.B. $P = \mathbb{P}$ für $R = \mathbb{Z}$).
Existenz der Primzerlegung für $a \in R$ $(a \neq 0)$

I Fall: $a \in R^\times$, Primzerlegung $a = e(a), \forall p \in P$: $v_p(a) = 0$

II Fall: a irreduzibel $\Rightarrow p = a_{\mathrm{nor}} \in P$, $a = ea_{\mathrm{nor}} = ep, e \in R^\times, e(a) := e, v_p(a) = \begin{cases} 1 & q = p \\ 0 & q \neq p \end{cases}$

Allgemeiner Fall wird durch Induktion nach $gr(a)$ bewiesen.
Es ist nur noch $a \in R, a \neq 0, a \notin R^\times, a$ nicht unzerlegbar zu betrachten $\Rightarrow a = u \cdot v$ mit u, v echte Teiler. Induktions-Hypothese mit Hilfe des Lemma 1.11 $\Rightarrow gr(u) < gr(a) \wedge gr(v) < gr(a)$, also haben u, v Primzerlegung $\Rightarrow$ (Durch Ausmultiplizieren) a hat Primzerlegung: $e(a) = e(u) \cdot e(v) \in R^\times$, $v_p(a) = v_p(u) + v_p(v)$

Eindeutigkeit: $a = e(a) \cdot \prod p^{v_p(a)} = e'(a) \cdot \prod p^{v'_p(a)}$ seien zwei Primzerlegungen.
Zu zeigen: $e(a) = e'(a), \forall p \in P : v_p(a) = v'_p(a)$
Induktion nach $n =: \sum_{p \in P}(v_p(a) + v'_p(a)) \in \mathbb{N}$
Induktionsanfang: $n = 0 \Rightarrow \forall p : v_p(a) = 0 = v'_p(a) \Rightarrow e(a) = e'(a)$
Induktionsschritt: $n > 0 \Rightarrow \exists p : v_p(a) > 0 \vee v'_p(a) > 0$, O.B.d.A.: $v_p(a) > 0 \Rightarrow p|a = e'(a) \prod_{q \in P} q^{v'_q(a)}$
Aus Lemma 1.12 leicht induktiv: $p|a_1 \cdot ... \cdot a_n \Rightarrow \exists j : p|a_j \Rightarrow \underbrace{p|e'(a)}_{\text{geht nicht}} \vee \exists q \in \mathbb{P} : p|q^{v'_q(a)} \Rightarrow p|q$
$\Rightarrow p$ ist normierter Teiler von $q \Rightarrow p = q$ ($p = 1$ geht nicht) $\Rightarrow p|p^{v'_p(a)} \Rightarrow v'_p(a) > 0$
$\tilde{a} = e(a)p^{v_p(a)-1} \prod_{q \neq p} p^{v_p(a)} = e'(a)p^{v'_p(a)-1} \prod_{q \neq p} q^{v'_p(a)}$
Zwei Primzerlegungen von $\tilde{a}$ mit $n-2$ statt n. Induktionshypothese anwendbar auf $\tilde{a} \Rightarrow e(a) = e'(a), \forall q \neq p : v_p(a) = v'_q(a)$. $v_p(a) - 1 = v'_p(a) - 1 \Rightarrow$ Induktionsschritt geleistet. ∎

Primzerlegung hat viele Anwendungen, z.B.: $\text{ggT}(a, b) = 1 \Rightarrow \text{ggT}(a^n, b^m) = 1$

Satz 1.13 (Irrationalitätskriterium)
Sei $\alpha \in \mathbb{C}$ eine Nullstellen von $f = X^m + \gamma_1 X^{m-1} + ... + \gamma_{m-1} X + \gamma_m \in \mathbb{Z}[X]$ (d.h. $\gamma_1, ..., \gamma_m \in \mathbb{Z}$) Ist dann $\alpha \notin \mathbb{Z}$, so $\alpha \notin \mathbb{Q}$.

Beweis
Annahme $\alpha \in \mathbb{Q}$, $\alpha = \frac{z}{n}, z \in \mathbb{Z}, n \in \mathbb{N}_+$, $\text{ggT}(z, n) = 1$
$0 = f(\frac{z}{n}) = \frac{z^m}{n^m} + \gamma_1 \frac{z^{m-1}}{n^{m-1}} + ... + \gamma_{m-1}\frac{z}{n} + \gamma_m$, multiplizieren mit $n^m \Rightarrow$
$0 = z^m + n \underbrace{(...)}_{\in \mathbb{Z}} \Rightarrow n|z^m \Rightarrow n|\text{ggT}(z^m, n) = 1$, da $\text{ggT}(z, n) = 1$ (s.o.)
$n|1 \Rightarrow \alpha = \frac{z}{n} = z \in \mathbb{Z}$. ∎

Anwendung: z.B. auf $f = X^k - a, a \in \mathbb{Z}(k > 1)$. Ist a keine k-te Potenz in $\mathbb{Z}, \alpha$ eine Nullstelle von f in $\mathbb{C}$ (sozusagen $\alpha = \sqrt[k]{a}$), so ist α irrational.

[$\alpha \in \mathbb{Z} : a = \alpha^k$ ist k-te Potenz in $\mathbb{Z}$] Tritt zum Beispiel ein, wenn $\exists p \in \mathbb{P} : k \nmid v_p(a)$ (denn $a = z^k \Rightarrow v_p(a) = k \cdot v_p(z)$. Etwa $\sqrt[k]{q}, q \in \mathbb{P}$ ist immer irrational, z.B. $\sqrt{2}$.

Die erste Grundlagenkrise der Mathematik Die Pythagoräer glaubten, alle Naturwissenschaften seien durch $\mathbb{N}$ „mathematisierbar“. Zum Beispiel wurde Folgendes als selbstverständlich betrachtet:
Man kann kleinen Einheitsmaßstab e (verdeutlicht durch einen gezeichneten Streckenstab mit kleinen Einheiten) wählen, so dass die Strecke a und die Strecke b in der Form $a = n \cdot e, b = m \cdot e$ ist, mit $n, m \in \mathbb{N} \Leftrightarrow \frac{b}{a} \in \mathbb{Q}$.
Modern ist die Aussage $\frac{b}{a} = \sqrt{2} \Rightarrow$ Seite und Diagonale erfüllen nicht dem Glauben.

Der Glaube besagt: Nur natürliche und rationale Zahlen sind Zahlen. ⇒ Die Länge einer Strecke ist keine Zahl.

Der Dozent glaubt, dies hat die Griechen daran gehindert „reelle Zahlen“ zu erfinden, d.h. mit Längen von Strecken wie in einem Körper zu rechnen (wirkt über 1000 Jahre, relle Zahlen exakt erst seit ca. 1800 exakt erklärt!).
Heute bekannt: Die Proportionenlehre von Eudoxos von Knidos ist logisch äquivalent zu der Konstruktion der rellen Zahlen.