Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K2: Grundlagen aus der elementaren Zahlentheorie

Stichworte: Klären/Vereinheitlichen von Notation, Wiederholung von ZT-Grundlagen,
speziell: Def. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, g-adische Darstellung / $g=2$: Binärsystem,
Def. Gruppe / Ring / Körper, Teilbarkeit
Def. ggT, teilerfremd, PFZ, Eind. der PFZ $\rightsquigarrow$ Faktorisierungsproblem
ggT: Div. mit Rest / Euklid. Algo mit Erweiterung (↦ Bézout-El.),
Kongruenzenrechnen, Invertieren in $\mathbb{Z}_m^\times$ mit euklid. Algo, CRS, modulare Brüche

2.1. **Einleitung:** Wir einigen uns auf Notation bestimmter Grundkonstrukte der Zahlentheorie, die Darstellung von Zahlen, und wiederholen dafür Grundlagen aus den Grundvorlesungen. Der Fokus wird auf die algorithmische Machbarkeit gelenkt.

2.2. 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 $\cdot$ sind verschiedene Axiome erfüllt, die diese (unendlichen) 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 $+,\cdot$ verträgt. Für $\mathbb{C}$ ist eine solche Anordnung nicht mehr möglich. ($i^2 = -1 < 0$, ↯ zu "$-$" "mal" "$-$" gibt "$+$")

Wir erinnern an die Definitionen:

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

2.4. **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 $-g$).

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

2.6. **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" →

2.7. **Bem.:** Die Addition $+$ ist in einem Ring stets kommutativ. [Vgl. LA1, L7.16 (i)]
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.

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

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

Algebraische Strukturen dieser Art können wir auch in Teilmengen von $\mathbb{Z}$ auffinden und diese für kryptographische Anwendungen ausnutzen. Dabei wird klar, dass die Anwendungen auch - teilweise - in beliebigen Gruppen / Ringen / Körpern möglich sind.
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:

2.10. **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.
⌜Bew. s. EinfZT, EZ 6.2⌟

2.11. **Def.:** Die Ziffernfolge $c_k, c_{k-1}, \dots, c_0$ heißt g-adische Darstellung von n.
Die Zahl c_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.

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

Bsp.: $163_{(10)} = 1 \cdot 10^2 + 6 \cdot 10^1 + 3 \cdot 10^0$,
$43_{(10)} = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 101011_{(2)}$
$= 2 \cdot 16^1 + 11 \cdot 16^0 = 2B_{(16)}$

2.13. 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 mit Laufzeit $O(n \log(n) \operatorname{loglog}(n))$ ⌜naiv: $O(n^2)$, Karatsuba-Algo: $O(n^{\log_2(3)})$; Schö/Stra besser als Karatsuba ab einigen 1000 Stellen⌟
↳ für n-stellige Zahlen

2.14. Die Länge von n in Satz 2.10 ist gleich $\lfloor \frac{\log(n)}{\log(g)} \rfloor + 1$, worin $\lfloor x \rfloor := \max\{k \in \mathbb{Z} : k \le x\}$ die Gaußklammer von x bezeichne.
⌜Denn: $g^k \le n < g^{k+1} \Leftrightarrow k \le \frac{\log(n)}{\log(g)} < k+1 \Leftrightarrow k = \lfloor \frac{\log(n)}{\log(g)} \rfloor$.⌟
Soviele Ziffern müssen zum Hinschreiben/Eintippen von n angegeben werden.
Diese Ziffernanzahl gibt die Inputgröße/Eingabegröße an.
Bei verschiedenen Basen ändert sich hier nur der Faktor $\frac{1}{\log(g)}$ vor $\log(n)$.
Deswegen sagt man, die Länge $k+1$ 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"
↳ Zur Landau-Symbolik vgl. Vorlesung "Anal. ZT", AnZ3.

Grundlegend für das Studium von $\mathbb{Z}$ ist der Begriff der Teilbarkeit:

2.15. 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 $a \nmid b$.

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

2.17. 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:

2.18. 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. ⌜Bew. s. EZ 2.14⌟

2.19. 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. $p^{e_i} \mid n$, aber $p^{e_i+1} \nmid n$. 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.
Zählt man die Primteiler gemäß ihrer Vielfachheit/Multiplizität in der PFZ von n, so zählt man die Anzahl der Primfaktoren von n.
Diese ist $\Omega(n) := \sum_{p \mid n} \max\{e \in \mathbb{N};\ p^e \mid n\}$.
Man schreibt auch $\omega(n) = \sum_{p \mid n} 1$ und $\Omega(n) = \sum_{p^{e(p)} \| n} e(p)$.
Ist $n = p_1^{e_1} \cdots p_r^{e_r}$, ist also $\omega(n) = r$ und $\Omega(n) = \sum_{i=1}^{r} e_i$.

2.20. Bsp.: die PFZ von 360 ist $360 = 2^3 \cdot 3^2 \cdot 5^1$, d.h. $e(2) = 3$, $e(3) = 2$, $e(5) = 1$, und sonst $e(p) = 0$ für $p \notin \{2,3,5\}$.
Haben $\omega(360) = 3$, $\Omega(360) = 3 + 2 + 1 = 6$.

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, vgl. K4) beruhen:

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

2.22. Bsp.: $F_5 = 2^{2^5} + 1$ ist durch 641 teilbar (Euler 1732)
$2^{2^5} + 1 = 641 \cdot 6\,700\,417$)

2.23 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.

2.24. Das derzeit schnellste algorithmische Verfahren zur Faktorisierung (auf einem klassischen Computer) ist das Zahlkörpersieb (vgl. K9) 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 $\log n$; $\exp(C(\log n)^{1/3}(\log\log n)^{2/3})$: irgendwo dazwischen...; $\exp(D\log n)$: exponentiell in $\log n$)
[Inputgröße: $O(\log n)$] vgl. 2.14

2.25. P. Shor entdeckte um 1994, dass das Faktorisierungsproblem auf einem Quantencomputer mit einer Laufzeit von (meist) nur $O((\log n)^{3/2})$ sehr schnell (d.h. polynomiell) gelöst werden kann, was die Sicherheit gängiger Kryptoverfahren wie RSA untergräbt. Allerdings ist die Konstruktion solcher Quantencomputer (physikalisch) extrem schwierig, diverse Forschergruppen verschiedener Regierungen, Forschungsorganisationen, großer Computer- und Technologiefirmen arbeiten daran. Mehr zu Quantencomputing in K10–K12.

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

2.26. 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 die PFZ aber so nicht praktisch zur ggT-Berechnung benutzt werden. Stattdessen benutzt man den (polynomiell) schnellen euklidischen Algorithmus in 2.28, der die Laufzeit $O(\log(\min(|a|,|b|)))$ hat, vgl. Satz von Lamé, EinfZT, EZ 5.13.

2.27. **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).

$\lfloor \cdot \rfloor$: Gauß-Klammer

Bsp.: $20 = 7 \cdot 2 + 6 = 7 \cdot 3 + (-1)$
(↑ kl. nn. Rest, ↑ abs. kl. Rest)

[EinfZT, EZ 1.7]

2.28. **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 $ggT(a,b) = xa + yb$ (ganz Schema ↑ ("Erweiterter Eukl. Algo")

Beschreibung des Rechenverfahrens: (a, b)

Letzte Division: $r_{m-1} = q_m r_m$

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

Schematisch:

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

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

q_k			4	3	$2 = m$
c_k	0	1	4	13	$30 = \frac{360}{12}$
d_k	1	0	1	3	$7 = \frac{84}{12} \rightsquigarrow \underbrace{13}_{y} \cdot 84 - \underbrace{3}_{x} \cdot 360 = 12$

Es gilt 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.: EinfZT, EZ 3.7, EZ 4.19]

Wiederholung zum Restklassenrechnen:

2.29. **Def.:** Sei $m \in \mathbb{N}$. Dann heißen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ kongruent modulo m, wenn $m \mid (b-a)$. Kurz: $a \equiv b \bmod m$ oder $a \equiv b \ (m)$.
Die Zahl m heißt Modul der Kongruenz.
Die Äquivalenzklassen von $\equiv$ modulo m heißen Restklassen modulo m.
(auch: Kongruenzklassen modulo m).

2.30. **Folgerungen:** Die Restklassen modulo m sind Teilmengen von $\mathbb{Z}$ der Gestalt $x + m\mathbb{Z} := \{x + ma ; a \in \mathbb{Z}\}$.
Die Restklasse $x + m\mathbb{Z}$ heißt auch die Restklasse von x modulo m.
Davon gibt es m Stück; wird in jeder Restklasse ein Element x_i, $i = 1, \dots, m$, ausgewählt, können die m Restklassen mit $x_1 + m\mathbb{Z}, x_2 + m\mathbb{Z}, \dots, x_m + m\mathbb{Z}$ angegeben werden; die Menge $\{x_1, \dots, x_m\}$ heißt dann vollständiges Restsystem modulo m. Sind $y_1, \dots, y_m \in \mathbb{Z}$ so, dass $y_i \not\equiv y_j \bmod m$ für alle $i \neq j$, $1 \leq i, j \leq m$, gilt (d.h. sind die y_i paarweise inkongruent modulo m), dann ist $\{y_1, \dots, y_m\}$ ein vollständiges RS mod m.

2.31. **Folgerungen:** Ist $\{x_1, \dots, x_m\}$ ein voll. RS mod m und $a \in \mathbb{Z}$, $c \in \mathbb{Z}$ mit $ggT(c, m) = 1$, so sind auch $\{x_1 + a, \dots, x_m + a\}$ und $\{x_1 \cdot c, \dots, x_m \cdot c\}$ voll. RSe mod m.

2.32. **Def.:** Ist der Modul $m \in \mathbb{N}$ klar, schreiben wir auch $\underline{x} := x + m\mathbb{Z}$ für die Restklasse von x mod m.
Wir definieren für $x, y \in \mathbb{Z}$ dann $\underline{x} + \underline{y} := \underline{x+y}$ und $\underline{x} \cdot \underline{y} := \underline{x \cdot y}$, d.h. $(x + m\mathbb{Z}) + (y + m\mathbb{Z}) := (x + y) + m\mathbb{Z}$. Dies erklärt "+", "·".
Weiter sei $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m := \{x + m\mathbb{Z} ; x \in \mathbb{Z}\}$ die Menge der (m vielen) Restklassen modulo m.
Die Operationen +, · sind wohldefiniert.

2.33. **Satz:** Zu $\underline{x} \in \mathbb{Z}_m$ ex. genau dann ein multiplikatives Inverses, d.h. ein $\underline{y} \in \mathbb{Z}_m$ mit $\underline{x} \cdot \underline{y} = \underline{1} \Leftrightarrow x \cdot y \equiv 1 \ (m)$, falls $ggT(x, m) = 1$.
Wir schreiben dann $\underline{x}^{-1}$ oder $\underline{x}^*$ für $\underline{y}$.

Bew.: Nimm $a := m$, $b := x$ im erkl. Alg. 2.28. $\rightsquigarrow 1 = ggT(a,b) = (-1)^{n-1} d_{n-1} \underbrace{a}_{=m} + (-1)^n c_{n-1} \underbrace{b}_{=x}$,
daran ablesbar: $x^{-1} \equiv (-1)^n c_{n-1} \pmod m$. □

2.34. **Fazit:** Mit dem euklidischen Algorithmus können wir Inverse schnell explizit berechnen.
Bsp.: Gesucht: $7^{-1} \bmod 37$, haben: $37 = 5 \cdot 7 + 2$, $7 = 3 \cdot 2 + 1$, $2 = 2 \cdot 1 + 0$

		$k=0$	$k=1$	$k=2$	
q_k		5	3	2	
c_k	0	1	5	16	37

$\rightsquigarrow +16 \equiv 7^{-1} (37)$
Probe: $16 \cdot 7 = 112 = 1 + 3 \cdot 37$

2.35. **Def.:** $\underline{x} = x + m\mathbb{Z}$ heißt prime oder reduzierte Restklasse mod m, falls $ggT(x,m) = 1$ gilt. Diese sind genau die Einheiten in $(\mathbb{Z}_m, +, \cdot)$, d.h. $\mathbb{Z}_m^\times = \{\underline{x} \in \mathbb{Z}_m ; ggT(x,m) = 1\}$.
Die Anzahl der Einheiten sei $\varphi(m) := \# \mathbb{Z}_m^\times = \#\{a \in \mathbb{N} ; a \le m, ggT(a,m) = 1\}$, die so erklärte Fkt. $\varphi : \mathbb{N} \to \mathbb{N}$ heißt Eulersche φ-Funktion.
Jedes Repräsentantensystem $\{x_1, \dots, x_{\varphi(m)}\}$ von $\mathbb{Z}_m^\times$ heißt reduziertes Restsystem modulo m.

2.35. Berechnung der φ-Funktion: $\varphi(p^a) = p^a - p^{a-1}$, $\varphi(p_1^{e_1} \cdots p_r^{e_r}) = \prod_{i=1}^{r} (p_i^{e_i} - p^{e_i - 1}) = m \prod_{p \mid m} (1 - \frac{1}{p})$,
denn φ ist multiplikativ laut CRS 2.37 (d.h., dass $\varphi(mn) = \varphi(m)\varphi(n)$ für $(m,n) = 1$ gilt).

2.36. Folgerungen: $(\mathbb{Z}_m^\times, \cdot)$ ist eine Gruppe, die multiplikative Gruppe von $\mathbb{Z}_m$, und die Gruppe $(\mathbb{Z}_m, +)$ heißt additive Gruppe von $\mathbb{Z}_m$.
Wir nennen $(\mathbb{Z}_m, +, \cdot)$ den Restklassenring mod m.
Im Fall wenn $\mathbb{Z}_m^\times = \mathbb{Z}_m \setminus \{0\}$ ist, ist $(\mathbb{Z}_m, +, \cdot)$ ein Körper; dies ist genau dann richtig, wenn $m = p$ eine Primzahl ist, weil genau dann alle $1, 2, \dots, m-1$ zu m teilerfremd sind. Wir bezeichnen für p prim diesen Körper mit p Elementen mit $\mathbb{F}_p$ (weitere endliche Körper ex. laut Algebra A 21.5 zu jeder Primpotenz p^a, genannt $\mathbb{F}_{p^a}$, als Zerfällungskörper des Polynoms $T^{p^a} - T \in \mathbb{F}_p[T]$. Dann hat $\mathbb{F}_{p^a}$ genau p^a viele Elemente. Allerdings ist $\mathbb{F}_{p^a}$ für $a \ge 2$ nicht zu $\mathbb{Z}/p^a$ isomorph (der (als Ring) Nullteiler hat: $p \cdot p^{a-1} = 0$).
In dieser Vorlesung werden wir teilweise konkret mit solchen Körpern arbeiten (und dafür z.T. auch explizit konstruieren, damit die Operationen "+", "·" auf dem Rechner realisierbar sind).

Die Struktur der Restklassenringe $(\mathbb{Z}_m, +, \cdot)$ versteht man besser, indem man sie auf "kleinere" Ringe zurückführt. Dies leistet der "CRS":

2.37. **Chinesischer Restsatz** (Restklassenring-Version, vgl. Algebra A12.4):
Sei $m > 1$ eine natürliche Zahl und $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$ eine Zerlegung von m in paarweise teilerfremde Zahlen $m_i > 1$.
Dann ist die Abbildung $F: \mathbb{Z}/m\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})$
$x + m\mathbb{Z} \mapsto (x + m_1\mathbb{Z}, \ldots, x + m_r\mathbb{Z})$
ein Ringisomorphismus, d.h. ein bijektiver Ringhomomorphismus.

Für die Restklassen bedeutet dies Konkreter:

2.38. **Chinesischer Restsatz** (Simultane Kongruenzen-Version):
Seien $m_1, \ldots, m_r > 1$ paarweise teilerfremde Zahlen, und seien $a_1, \ldots, a_r \in \mathbb{Z}$. Dann ist das simultane Kongruenzensystem
$x \equiv a_1 \bmod m_1, \quad x \equiv a_2 \bmod m_2, \ldots, x \equiv a_r \bmod m_r$
in x lösbar, die Lösungen sind alle kongruent modulo $m_1 \cdots m_r$.

2.39. **Bem.:** Aus Version 2.37 folgt Version 2.38 wegen der Bijektivität von F, denn $(a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z})$ hat dann genau ein Urbild $x + m\mathbb{Z}$. □

2.40. **Zusatz zum CRS** (= chinesischer Restsatz) in Variante 2.38:
Genau alle $x \equiv x_0 \bmod m_1 \cdots m_r$ lösen das System, wobei $x_0 = a_1 M_1^\times M_1 + \ldots + a_r M_r^\times M_r$, wo $M_i := \frac{m_1 \cdots m_r}{m_i}$ $(i = 1, \ldots, r)$ und $M_i^\times \in \mathbb{Z}$ ein multiplikatives Inverses von M_i mod m_i repräsentiert $(i = 1, \ldots, r)$, d.h. es gilt $M_i^\times \cdot M_i \equiv 1 \bmod m_i$, wobei die $M_i^\times$ mit dem euklidischen Algorithmus wie in 2.33/34 (schnell) berechnet werden können.

Fall $r = 2$: $M_1 = m_2$ und $M_2 = m_1$ teilerfremd heißt $1 = ggT(M_1, M_2) = x m_2 + y m_1$ mit Bezout-El. x, y, hier die $x \equiv m_2^{-1}(m_1)$, $y \equiv m_1^{-1}(m_2)$ gilt, also $M_1^\times = x$, $M_2^\times = y$.

2.41 **Bsp. zum CRS:** Das System $x \equiv 2\ (7),\ x \equiv 3\ (8)$ hat die Lösung $x \equiv \underbrace{2}_{\text{Inv. von } 8 \bmod 7} \cdot 1 \cdot 8 + \underbrace{3}_{\text{Inv. von } 7 \bmod 8} \cdot (-1) \cdot 7 = 16 - 21 = -5 \equiv 51 \mod 56$.

Also: $\left\{ \begin{array}{l} x \equiv 2\ (7) \\ \wedge\ x \equiv 3\ (8) \end{array} \right\} \Leftrightarrow x \equiv 51\ (56)$.

Bem.: $1 \equiv \bar{8}^{-1}\ (7)$, $-1 \equiv \bar{7}^{-1}\ (8)$ ist ablesbar an $1 = \underbrace{1}_{\text{Bezout-Ez. von } ggT(8,7)=1} \cdot 8 + (-1) \cdot 7$

2.42 **Bsp.:** Bei manchen zahlentheoretischen Aufgaben wie z.B. die Frage, ob es ganzzahlige Lösungen zu bestimmten Gleichungen geben kann, ist die "modulare Brille" ein nützliches Hilfsmittel, hier ein Bsp., wo wir die modulare Brille mod 8 aufziehen, um mehr zu sehen:

Betr. die Glg. $8x + 7 = u^2 + v^2 + w^2$ in $u, v, w, x \in \mathbb{N}_0$.

Sie ist unlösbar: Denn mod 8 erhalten wir $\bar{7} \equiv u^2 + v^2 + w^2\ (8)$;

z	0	± 1	± 2	± 3	4
z^2	0	1	4	1	0

← alle Quadrate mod 8

alle quadratischen Reste mod 8 sind 0, 1, 4,

daher ist $v^2 + w^2 \equiv 0, 1, 4, 2, 5\ (8)$,

also $u^2 + v^2 + w^2 \equiv 0, 1, 4, 2, 5,\ 1, 2, 5, 3, 6,\ 4, 5, 0, 6, 1\ (8)$,

d.h. $u^2 + v^2 + w^2 \equiv 0, 1, 2, 3, 4, 5, 6\ (8)$, aber nie $\equiv 7\ (8)$.

Es kann keine Lösungen mod 8 geben, also auch keine in $\mathbb{Z}$.