Zahlentheorie ist die Mathematik der ganzen Zahlen.

Diophantische Gleichungen
Eine Gleichung der Form $ax + by = c$ mit $a, b, c \in \mathbb{N}$ und $x, y \in \mathbb{Z}$ heißt *diophantische Gleichung.*
In der Regel sind a, b, c gegeben und x, y gesucht.
Wir schreiben Lösungen als Zahlenpaar (x/y).

Teiler und Primzahlen
Definition:
(i) Es seien $x \in \mathbb{Z}, k \in \mathbb{N}$. k heißt *Teiler* von x, geschrieben $k|x$, falls es ein $q \in \mathbb{Z}$ gibt, so dass $x = k \cdot q$.
(ii) Seien $a, b \in \mathbb{N}$. Dann ist der *größte gemeinsame Teiler von* a, b definiert durch:
$\mathrm{ggT}(a, b) = \max\{k \in \mathbb{N} : k|a \wedge k|b\}$
(iii) Eine natürliche Zahl $p > 1$ heißt *Primzahl* oder *prim*, wenn sie genau zwei Teiler besitzt: die 1 und sich selbst.

Hauptsatz der Zahlentheorie
Jede natürliche Zahl $n > 1$ lässt sich, bis auf die Reihenfolge der Faktoren, eindeutig als Produkt von Primzahlen darstellen.

Folgerung: Jeder gemeinsame Teiler von a und b ist auch Teiler von $\mathrm{ggT}(a, b)$.

Satz: Seien $a, b, k \in \mathbb{N}, x, y \in \mathbb{Z}$. Dann gilt:
Aus $k|a$ und $k|b$ folgt $k|(ax + by)$.

Satz: Seien $a, b, c \in \mathbb{N}$, $x, y \in \mathbb{Z}$. Dann gilt:
Besitzt die Gleichung $ax + by = c$ eine Lösung (x/y), so folgt: $\mathrm{ggT}(a, b)|c$.

Satz: (Teilen mit Rest) Seien $a, b \in \mathbb{N}$.
Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{N}_0$ mit: $a = q \cdot b + r$ und $0 \leq r \leq b - 1$

Satz: Seien $a, b \in \mathbb{N}, q, r \in \mathbb{N}_0$ und $a = q \cdot b + r$. Dann gilt:
$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$

Satz: (Erweiterter Euklidscher Algorithmus)
$\forall a, b \in \mathbb{N}\, \exists x, y \in \mathbb{Z} : ax + by = \mathrm{ggT}(a, b)$

Satz: (Lösungen diophantischer Gleichungen)
Gegeben sei die diophantische Gleichung $ax + by = c$ mit $\mathrm{ggT}(a, b)|c$. Dann gilt:
(i) Es gibt mindestens eine Lösung (x_0, y_0)
(ii) Ist (x_0, y_0) eine Lösung, dann sind auch alle Zahlenpaare $(x_0 + kb/y_0 - ka)$ mit $k \in \mathbb{Z}$ Lösungen.
(iii) Gilt $\mathrm{ggT}(a, b) = 1$, dann sind durch (ii) alle Lösungen gegeben.

Kongruenz
Definition: Seien $a, b \in \mathbb{Z}, m \in \mathbb{N}$.
Dann heißt *a kongruent zu b modulo m*, falls $a - b$ durch m teilbar ist.
Wir schreiben dann: $a \equiv b \mod m$.

Satz: Folgende Aussagen sind äquivalent:
(1) $a \equiv b \mod m$.
(2) $\exists k \in \mathbb{Z} : a = b + k \cdot m$
(3) Beim Teilen mit Rest a durch m, b durch m bleibt derselbe Rest.

Satz: Die Relation *kongruent modulo m* ist eine Äquivalenzrelation auf $\mathbb{Z}$.
(1) $a \equiv a \mod m$ (Reflexivität)
(2) $a \equiv b \mod m \Rightarrow b \equiv a \mod m$ (Symmetrie)
(3) $a \equiv b \mod m$ und $b \equiv c \mod m \Rightarrow a \equiv c \mod m$ (Transitivität)

Satz: (Rechenregeln für Kongruenzen)
Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann gilt:
(1) $-a \equiv -b \mod m$
(2) $a + c \equiv b + d \mod m$
(3) $a \cdot c \equiv b \cdot d \mod m$
(4) $a^2 \equiv b^2 \mod m, a^3 \equiv b^3 \mod m$, etc.

Restklassen
Definition: Die *Restklasse* $\overline{a}$ *von* a *modulo* m ist definiert durch:
$\overline{a} := \{b \in \mathbb{Z} : b \equiv a \mod m\}$
Andere Schreibweise für die Restklasse $\overline{a}$: $[a]$

Rechnen im Restklassenring
Definition: Seien $a, b \in \mathbb{Z}$.
$\overline{a} + \overline{b} := \overline{a+b}$
$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$

Satz: (Satz vom Dividieren)
Ist p eine Primzahl und sind $a \in \mathbb{Z}, b \in \{1, ..., p-1\}$, so besitzt die Gleichung
$\overline{b} \cdot \overline{x} = \overline{a}$ in $\mathbb{Z}_p$ genau eine Lösung $\overline{x}$, d.h. $\frac{\overline{a}}{\overline{b}}$ ist definiert.

Merkregel:
Wenn wir $\frac{\overline{1}}{\overline{a}}$ in $\mathbb{Z}_m$ suchen, dann lösen wir die diophantische Gleichung $ax + my = 1$.
Es gilt dann: $\frac{\overline{1}}{\overline{a}} = \overline{x}$

Der kleine Satz von Fermat:
Sei p Primzahl, $a \in \mathbb{N}$ kein Vielfaches von p. Dann gilt:
$a^{p-1} \equiv 1 \mod p$

Primitivwurzel
Definition: Ein Element $\overline{g} \in \mathbb{Z}_m$ heißt *Primitivwurzel*, falls durch $\overline{g}^k$ alle Elemente von $\mathbb{Z}_m$ außer $\overline{0}$ dargestellt werden können.

Diffie-Hellman Schlüsselaustausch
Alice und Bob vereinbaren Primzahl p und $g \in \{1, ..., p-1\}$ (am besten eine Primitivwurzel).
Alice wählt geheim eine Zahl a aus, Bob geheim eine Zahl b mit $a, b \in \{1, ..., p-1\}$.
Alice berechnet $A = g^a \mod p$, Bob berechnet $B = g^b \mod p$.
Dann tauschen Sie A und B aus. Öffentlich bekannt sind also p, g, A, B.
Beide können nun den gemeinsamen Schlüssel K berechnen:
Alice rechnet $K = B^a \mod p$, Bob rechnet $K = A^b \mod p$

RSA-Verfahren
Alice wählt zwei Primzahlen p, q und berechnet $m = p \cdot q$ und $\tilde{m} = (p-1)(q-1)$.
Alice wählt Verschlüsselungsexponent e mit $1 < e < \tilde{m}$ und $\mathrm{ggT}(e, \tilde{m}) = 1$.
Alice berechnet den Entschlüsselungsexponent d mit: $e \cdot d \equiv 1 \mod \tilde{m}$
(m, e) ist der öffentliche Schlüssel, (m, d) der private Schlüssel von Alice.
Bob verschlüsselt die Nachricht $n, (0 < n < m)$: $N = n^e \mod m$
Alice entschlüsselt die Nachricht: $n = N^d \mod m$