Verschlüsselung der elektronischen Post

Im folgenden soll *Pretty Good Privacy* (PGP) rudimentär untersucht werden. Dazu wird kurz eine Möglichkeit, die dem Benutzer mit PGP zur Verfügung steht, beschrieben und anschließend auf das zentrale Verschlüsselungsverfahren dieser Kombination näher eingegangen.

RSA, in Kombination mit MD5 und IDEA, sind jedoch nicht die einzigen Verfahren, die PGP verwendet. Es würde allerdings den Rahmen dieser Einführung sprengen, auf alle Möglichkeiten, die dem Benutzer zur Verfügung stehen (DH/DSS statt RSA; CAST, IDEA oder 3DES zur Verschlüsselung und SHA als Ersatz für MD5), einzugehen. Ich werde mich folglich im nächsten Abschnitt auf die Erklärung des RSA-Algorithmus beschränken.

Der MD5-Algorithmus (*Message-Digest*) bildet eine 128-Bit lange Quersumme aus einer beliebig langen Nachricht. Der RSA-Algorithmus wird auf diese Quersumme angewendet, um die digitale Unterschrift zu erzeugen.

Der IDEA-Algorithmus (*International Data Encryption Algorithm*) verwendet für jede E-Mail einen neuen, zufällig erzeugten 128-Bit Schlüssel, mit dem die Nachricht chiffriert wird.

Und jetzt zu den einzelnen Punkten in Tabelle 1.

Digitale Unterschrift

Die digitale Unterschrift wird wie folgt eingesetzt:

1. Der Sender erzeugt eine Nachricht.
2. Mit Hilfe von MD5 wird eine 128-Bit lange Quersumme der Nachricht erzeugt.
3. Die Quersumme wird mit dem RSA-Algorithmus verschlüsselt, wozu der private Schlüssel des Senders benutzt wird. Das Ergebnis wird der Nachricht vorangestellt.
4. Der Empfänger entschlüsselt mit dem öffentlichen Schlüssel des Senders mit Hilfe von RSA die digitale Unterschrift und erhält so wieder die Quersumme.
5. Der Empfänger erzeugt mit MD5 eine neue Quersumme und vergleicht beide. Sind sie identisch, so ist die Nachricht authentisch.

Vertraulichkeit

Vertraulichkeit wird durch die Verschlüsselung der Nachricht vor ihrer Übertragung hergestellt. Dazu wird die Nachricht mit Hilfe des IDEA-Algorithmus verschlüsselt. Der dazu notwendige konventionelle Schlüssel wird nur einmal verwendet. Für jede Nachricht

Funktion	**Algorithmus**	**Beschreibung**
Chiffrierung der Nachricht	**IDEA, RSA**	Die Nachricht wird mit dem IDEA-Algorithmus verschlüsselt. Dazu wird ein Einwegschlüssel (*one time session key*) vom Sender erzeugt. Dieser Einwegschlüssel wird mit dem öffentlichen Schlüssel des Empfängers mit Hilfe des RSA-Algorithmus verschlüsselt und der Nachricht vorangestellt.
Digitale Unterschrift	**MD5, RSA**	Mit MD5 wird eine Quersumme (*hash code*) der Nachricht erzeugt. Diese wird anschließend mit dem privaten Schlüssel des Senders mit Hilfe des RSA-Algorithmus verschlüsselt und der Nachricht vorangestellt.
Kompression	**ZIP**	Die Nachricht kann vor dem Versenden mit ZIP komprimiert werden.
E-Mail Kompatibilität	**base64**	Eine verschlüsselte Nachricht kann mit base64 nach ASCII konvertiert werden.

Tabelle 1: Zusammenfassung der PGP-Dienste

wird also ein neuer, zufällig erzeugter 128-Bit Schlüssel benötigt. Damit die Nachricht beim Empfänger wieder entschlüsselt werden kann, muß der Schlüssel mit übertragen werden. Um ihn vor Angriffen zu schützen, wird er vorher mit dem öffentlichen Schlüssel des Empfängers chiffriert.

Es ergibt sich folgender Ablauf:

1. Der Sender erzeugt die Nachricht und einen zufälligen 128-Bit Schlüssel, der nur für diese Nachricht verwendet wird (Einwegschlüssel).
2. Die Nachricht wird verschlüsselt, wozu der IDEA-Algorithmus mit dem Einwegschlüssel verwendet wird.
3. Der Einwegschlüssel wird mit dem öffentlichen Schlüssel des Empfängers mit dem RSA-Algorithmus verschlüsselt und der Nachricht vorangestellt.
4. Der Empfänger verwendet RSA und seinen privaten Schlüssel, um den Einwegschlüssel zu dechiffrieren.
5. Mit Hilfe des Einwegschlüssels entschlüsselt er dann die Nachricht.

Vertraulichkeit und digitale Unterschrift

Beide Dienste können natürlich auch zusammen verwendet werden. Dazu wird zunächst eine digitale Unterschrift mit dem privaten Schlüssel des Senders erzeugt und der Nachricht vorangestellt. Danach wird die Nachricht zusammen mit der digitalen Unterschrift mit dem IDEA-Algorithmus unter Verwendung des Einwegschlüssels chiffriert. Der Einwegschlüssel wird dann mit dem RSA-Algorithmus und dem öffentlichen Schlüssel des Empfängers chiffriert und der Nachricht vorangestellt.

Kompression

PGP komprimiert die Nachricht automatisch vor der Verschlüsselung, nachdem die digitale Unterschrift hinzugefügt wurde. Der Hauptgrund, warum die Quersumme und die digitale Unterschrift vor der Kompression gebildet werden müssen ist das nichtdeterministische Ergebnis des Kompressionsalgorithmus. Je nach Implementierung können nämlich Unterschiede bei der Kompression auftreten. Für die Dekompression sind diese jedoch irrelevant, man erhält immer das korrekte Ergebnis. Würde man folglich die Quersumme und digitale Unterschrift nach der Kompression bilden, würde dies PGP auf einen einzigen Kompressionsalgorithmus beschränken, da sonst kein eindeutiges Ergebnis bei der Dekompression zu erzielen wäre.

Wird die komprimierte Nachricht verschlüsselt, so erhöht das die kryptographische Sicherheit, da die komprimierte Nachricht wesentlich weniger Redundanzen enthält als die ursprüngliche Textnachricht.

E-Mail Verträglichkeit

Wenn PGP verwendet wird, so ist wenigstens ein Teil der Nachricht verschlüsselt und damit ein 8-Bit Datenstrom, der nicht mehr RFC 822 (→ S.3) entspricht. Da nicht alle elektronischen Postsysteme dies tolerieren, bietet PGP eine Konvertierung nach MIME mit base64 an.

Allein zu PGP sind einige Bücher erschienen, ganz zu schweigen von den angeführten Algorithmen. Zu PGP sind insbesondere [4] und [8] zu empfehlen, die Algorithmen werden z.B. in [3] oder [5] behandelt. Es ist also auf diese Bücher verwiesen, wenn sich der Leser tiefer in die Materie einarbeiten möchte.

Da der RSA-Algorithmus derjenige ist, der dem ganzen Verschlüsselungsverfahren die notwendige Sicherheit gibt, soll er im folgenden genauer betrachtet werden. Da die verwendete Mathematik nicht vorausgesetzt werden kann, werden zuerst die relevanten Gesetze aus der Zahlentheorie angegeben und bewiesen.

Der Algorithmus von Rivest-Shamir-Adleman (RSA)

Die Höhere Mathematik des Ingenieurstudiums beinhaltet in der Regel keine Zahlentheorie. Der Informatiker muß sich damit auseinandersetzen und ist daher, zumindest auf diesem Gebiet, dem Ingenieur voraus. Um diese Diskrepanz in puncto modulare Arithmetik auszugleichen, folgen anschließend einige Betrachtungen zu diesem Thema. Die Absicht ist, dem Leser den RSA-Algorithmus zum Chiffrieren und Dechiffrieren von Nachrichten mit Hilfe von öffentlichen und privaten Schlüsseln näher zu bringen und ihn für ihn verständlich zu machen.

Etwas Zahlentheorie

Die Stärke des RSA-Verfahrens liegt in der Schwierigkeit, große Zahlen n in ihre Primfaktoren (in diesem Fall in ihre beiden Primfaktoren p und q) zu zerlegen. Es gibt zur Zeit keinen vernünftigen Algorithmus, der in der Lage wäre, Zahlen mit mehreren hundert Stellen in ihre beiden Primfaktoren zu zerlegen. Der beste bekannte Algorithmus schafft die Zerlegung einer Zahl n in einer Zeit proportional zu $L(n) = \exp\left[\sqrt{\ln n \cdot \ln(\ln n)}\right]$.

Dies hat zur Folge, daß mit heutiger Technik eine 100-stellige Zahl in ungefähr zwei Wochen, eine 150-stellige in zirka einem Jahr und eine 200-stellige, eine Rechenleistung von 10^{12} Operationen pro Sekunde vorausgesetzt, in tausend Jahren zerlegt werden könnte.

Da die Primzahlen eine wichtige Rolle beim RSA-Verfahren spielen, soll mit ihnen begonnen werden. Zuerst aber eine Definition.

Definition 1. Es seien $a, d \in \mathbb{Z}$, wobei $d \neq 0$ gilt. Dann ist d ein Divisor von a (oder a ein Vielfaches von d), wenn es ein $b \in \mathbb{Z}$ mit $a = bd$ gibt. Um zu zeigen, daß a von d geteilt wird, schreibt man $d|a$.

Beispiel.

$2|8$, wegen $8 = 4 \cdot 2$
$5| - 15$, wegen $-15 = -3 \cdot 5$
6 dividiert 17 nicht, da es keine ganze Zahl b mit $17 = b \cdot 6$ gibt

Satz 1. Die folgenden Beziehungen sind gültig:

1. $d|a$ und $a|b$ impliziert $d|b$ (Transitivität)
2. $d|1$, dann ist $d = \pm 1$
3. $d|a$ und $a|d$, dann ist $d = \pm a$
4. $d|a$ und $d|b$, dann $d|(ax + by)$ für beliebige ganze Zahlen x, y

Beweis. Stellvertretend soll 4 bewiesen werden. Die Annahme, daß $d|a$ und $d|b$ impliziert, daß es ganze Zahlen m, n gibt, mit $a = md$ und $b = nd$. Daraus folgt $ax + by = (md)x + (nd)y = (mx + ny)d$ und damit $d|(ax + by)$. $\square$

Das Konzept des Divisors führt zur Definition der Primzahl.

Definition 2. Eine ganze positive Zahl p wird Primzahl (prim) genannt, wenn ihre einzigen beiden Divisoren 1 und p sind. Da die 1 ausgeschlossen wird, fangen die Primzahlen mit $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \dots$ an. Hat eine Zahl drei und mehr Divisoren, so wird sie zusammengesetzt genannt. Jede ganze Zahl größer als 1 ist entweder prim oder zusammengesetzt, jedoch niemals beides. Die 1 ist weder prim noch zusammengesetzt.

Der größte gemeinsame Teiler d zweier positiver ganzer Zahlen a, b wird wie folgt definiert:

Definition 3. Sind a, b ganze Zahlen, so wird für ihren größten gemeinsamen Teiler (*greatest common divisor*) $\gcd(a, b)$ geschrieben. Die ganze positive Zahl $d = \gcd(a, b)$ ist größter gemeinsamer Teiler von a und b, wenn

1. $d|a$ und $d|b$ und
2. jeder weitere Divisor c von a und b auch d teilt.

Da d eine ganze positive Zahl sein soll, gilt $d = \gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$.

Beispiel. $\gcd(12, 8) = 4$ und $\gcd(12, 9) = 3$.

Es gibt eine weitere Definition für den größten gemeinsamen Teiler. Sie beruht auf der Linearkombination zweier ganzer Zahlen.

Satz 2. Sind a, b ganze positive Zahlen, dann ist ihr größter gemeinsamer Teiler $\gcd(a, b)$ die kleinste ganze positive Zahl, die als Linearkombination $ax + by$, mit $x, y \in \mathbb{Z}$, ausgedrückt werden kann.

Beweis. Die Menge $M = \{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$ hat zumindest das Element $a^2 + b^2$ und ist somit nicht leer. M ist folglich eine nicht leere Untermenge von $\mathbb{N}$ und hat somit ein kleinstes Element $d = ax_1 + by_1$, mit $x_1 \in \mathbb{Z}$ und $y_1 \in \mathbb{Z}$ (sie ist wohlgeordnet).

Jetzt ist nur noch zu zeigen, daß $d = \gcd(a, b)$ ist. Wenn $d|a$, so gilt allgemein $a = qd + r$, mit $q \in \mathbb{Z}$ und $0 \leq r < d$. Dabei ist q der Quotient und r der Divisionsrest (siehe nächster Abschnitt). Es ist also $r = a - qd = a - q(ax_1 + by_1) = a(1 - qx_1) + b(-qy_1)$. Damit ist

$r \in M$. Da aber $r < d$ ist, ergibt sich ein Widerspruch zur Annahme, daß d das kleinste Element von M ist. Es muß also $r = 0$ und damit $a = qd$ sein, womit $d|a$ bewiesen wäre. Die gleiche Argumentation gilt für $d|b$.

Als nächstes ist zu zeigen, daß wenn $c|a$ und $c|b$ auch $c|d$. Angenommen, $c|a$ und $c|b$, dann gibt es ganze Zahlen m und n mit $a = cm$ und $b = cn$. Es folgt $d = ax_1 + by_1 = cmx_1 + cny_1 = (mx_1 + ny_1)c$, das heißt, $c|d$. □

Beispiel.

> $\gcd(3, 5) = 1$. Daher gilt $1 = 3 \cdot 2 + 5 \cdot (-1)$.
>
> $\gcd(10, 35) = 5$. Die Linearkombination lautet: $5 = 10 \cdot (-3) + 35 \cdot 1$. Satz 2 besagt, daß es keine kleinere positive ganze Zahl als 5 gibt (1, 2, 3 oder 4), die durch eine Linearkombination von 10 und 35 ausgedrückt werden kann.

Definition 4. Zwei positive ganze Zahlen a, b werden teilerfremd (relativ prim) genannt, wenn für sie $\gcd(a, b) = 1$ gilt.

Aus der Definition folgt unmittelbar

Satz 3. Wenn a und b ganze Zahlen ungleich Null sind und p eine Primzahl mit $p|ab$, so folgt $p|a$ oder $p|b$.

Beweis. Wenn $p|a$, dann ist die Aussage bewiesen. Wenn p nicht a dividiert, so sind beide teilerfremd und es gilt $\gcd(a, p) = 1$, bzw. $1 = ax + py$ mit $x, y \in \mathbb{Z}$. Multipliziert man nun die Gleichung mit b, so folgt $b = (ab)x + p(by)$. Da aber $p|ab$ und $p|p$ muß $p|b$. □

Wenn also p eine Primzahl ist und das Produkt zweier ganzer Zahlen ungleich Null dividiert, so muß es wenigstens eine der beiden Zahlen teilen. Dies läßt sich auf das Produkt von mehr als zwei ganzen Zahlen erweitern.

Satz 4. Wenn $a_1, a_2, \ldots, a_n$ ganze Zahlen ungleich Null sind und p eine Primzahl mit $p|a_1a_2\cdots a_n$, so muß $p|a_i$ für irgendein i, $1 \leq i \leq n$.

Beweis. Der Beweis erfolgt mit vollständiger Induktion. $S(n)$ sei folgende Aussage: Wenn $p|a_1a_2\cdots a_n$, dann gibt es wenigstens ein i, $1 \leq i \leq n$, für das $p|a_i$ gilt. Für $S(1)$ heißt das, wenn $p|a_1$ dann $p|a_1$, was sicher stimmt.

Angenommen, $S(k)$ ist wahr. Jetzt muß noch bewiesen werden, daß $S(k+1)$ (also der Schritt von k nach $k+1$) ebenfalls wahr ist. Das heißt, es ist zu beweisen, daß wenn die Annahme wenn $p|a_1a_2\cdots a_k$ dann $p|a_i$ für $1 \leq i \leq k$, wahr ist, daß dann auch die Aussage wenn $p|a_1a_2\cdots a_ka_{k+1}$ dann $p|a_i$ für $1 \leq i \leq k+1$, stimmt.

Bei $p|(a_1a_2\cdots a_k)(a_{k+1})$ handelt es sich um ein Produkt von zwei ganzen Zahlen ungleich Null. Es gilt also Satz 3 und damit entweder $p|(a_1a_2\cdots a_k)$ oder $p|a_{k+1}$. Da $S(k)$ als wahr angenommen wird, folgt aus $p|(a_1a_2\cdots a_k)$ unmittelbar $p|a_i$ für $1 \leq i \leq k$. Wenn $p|a_{k+1}$ dann $p|a_i$ für $1 \leq i \leq k+1$. □

Obwohl der Beweis ziemlich großen Aufwand für eine relativ klare Aussage bedeutet, ist er wegen der angewendeten Methode der vollständigen Induktion interessant. Sie basiert auf der Weitergabe von Wahrheiten. Es wird gezeigt, daß Aussage $S(1)$ wahr ist, was meistens problemlos ist. Dann wird angenommen, daß Aussage $S(k)$ wahr ist und gezeigt, daß die Wahrheit an $S(k+1)$ „weitergegeben“ wird. Zusammen mit der Tatsache, daß die Wahrheitskette mit einer wahren Aussage $S(1)$ beginnt folgt, daß auch $S(n)$ wahr sein muß.

Dieser Abschnitt wird mit dem Fundamentaltheorem der Arithmetik beschlossen.

Satz 5. Jede ganze Zahl $a > 1$ kann eindeutig (bis auf die Reihenfolge der Faktoren) durch ein Produkt von einer oder mehreren Primzahlen dargestellt werden.

Beweis. Es sei $M = \{x \in \mathbb{N} | x > 1$ und x kann nicht als Produkt einer oder mehrerer Primzahlen ausgedrückt werden$\}$. Es gilt zu beweisen, daß M leer ist.

Angenommen, M ist nicht leer. Dann muß es ein kleinstes Element c geben (die Menge ist wohlgeordnet). c kann keine Primzahl sein, da sie sonst nicht in M enthalten wäre. Also gibt es ganze Zahlen c_1, c_2, $1 < c_1 < c$ und $1 < c_2 < c$, mit $c = c_1c_2$. c ist also eine zusammengesetzte Zahl. c_1 und c_2 sind auch nicht in M enthalten, da sie kleiner als c sind und c ja das kleinste Element von M ist. Da sie nicht zu M gehören, können sie durch Primzahlen dargestellt werden. Dies gilt dann auch für c, da es ja ein Produkt von c_1 und c_2 ist.

Jetzt muß noch gezeigt werden, daß die Darstellung eindeutig ist. Angenommen, $c = p_1p_2\cdots p_r = q_1q_2\cdots q_t$ und alle p_i und q_i sind Primzahlen. Nach dem Kürzen aller gleicher Faktoren bleibt $c = p_1p_2\cdots p_s = q_1q_2\cdots q_m$ mit $1 \leq s \leq r$ und $1 \leq m \leq t$.

Es gilt $p_1|p_1p_2\cdots p_s$ und damit $p_1|q_1q_2\cdots q_m$. Laut Satz 4 muß daher $p_1|q_\mu$, für irgendein μ, $1 \leq \mu \leq m$. Dies ist aber ein Widerspruch zu der Annahme, daß alle gemeinsamen Faktoren weggekürzt wurden. Die Darstellung ist folglich eindeutig und $M = \emptyset$. □

Beispiel. Die Primfaktorisierung von 280 ist $280 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 = 2^3 \cdot 5 \cdot 7$.

Die Primfaktorisierung erlaubt auch den größten gemeinsamen Teiler zweier ganzer Zahlen größer 1 zu bestimmen. Angenommen, es ist $\gcd(10, 36)$ gesucht. $10 = 2 \cdot 5$ und $36 = 2^2 \cdot 3^2$. Die einzigen Teiler von 10 sind also 2, 5 und $2 \cdot 5$, von 36 sind es 2, 2^2, 3, 3^2, $2 \cdot 3$, $2^2 \cdot 3$, $2 \cdot 3^2$ und $2^2 \cdot 3^2$. Damit folgt für den $\gcd(10, 36) = 2$.

Modulare Arithmetik

Im Mittelpunkt der modularen Arithmetik steht die Restklassenalgebra. Es werden also Divisionsreste von ganzen Zahlen $x \in \mathbb{Z}$ betrachtet. Dieser Rest kann wie folgt ausgedrückt werden:

$$x = y \underbrace{\lfloor x/y \rfloor}_{\text{Quotient}} + \underbrace{x \bmod y}_{\text{Rest}} \tag{1}$$

Bei „mod“ handelt es sich in diesem Fall um eine zweistellige (binäre) Operation, ebenso wie es die Addition oder Multiplikation sind. Diese gilt sowohl für positive als auch negative ganze Zahlen.

$$x \bmod y = x - y\lfloor x/y \rfloor, \quad \text{für } y \neq 0 \tag{2}$$

Beispiel.

$$\begin{aligned}
5 \bmod 3 &= 5 - 3\lfloor 5/3 \rfloor = 5 - 3\lfloor 1.6 \rfloor = 2 \quad \text{(siehe Abbildung 1)} \\
5 \bmod -3 &= 5 - (-3)\lfloor 5/(-3) \rfloor = 5 - (-3)\lfloor -1.6 \rfloor = 5 - (-3)(-2) = -1 \\
-5 \bmod 3 &= -5 - 3\lfloor -5/3 \rfloor = -5 - 3\lfloor -1.6 \rfloor = -5 - 3(-2) = 1 \\
-5 \bmod -3 &= -5 - (-3)\lfloor -5/(-3) \rfloor = -5 - (-3)\lfloor 1.6 \rfloor = -5 - (-3)(1) = -2
\end{aligned}$$

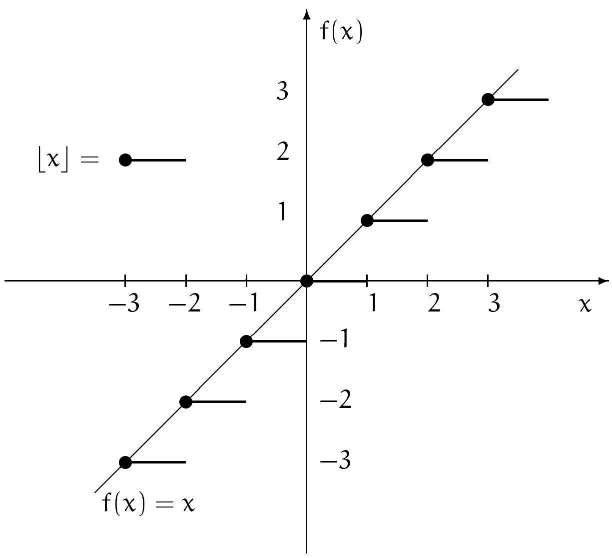

Abbildung 1: Rundungen auf ganze Zahlen

Wird „mod“ in Gleichungen verwendet, so empfiehlt sich eine etwas andere Schreibweise.

$$x \equiv y \pmod{n} \qquad \Longleftrightarrow \qquad x \bmod n = y \bmod n \tag{3}$$

Diese Schreibweise stammt von Gauß und wird „x kongruent y modulo n“ gelesen. Gauß schrieb dazu:

> *Numerorum congruentiam hoc signo,* $\equiv$, *in posterum denotabimus, modulum ubi opus erit in clausulis adiungentes,* $-16 \equiv 9 \pmod{5}$, $-7 \equiv 15 \pmod{11}$.

Eingedeutscht heißt „x kongruent y modulo n“ in etwa „x übereinstimmend (äquivalent, entsprechend) y mit dem Maß (gemessen an) n“.

Gemessen an heißt, daß die Rechnung in der Menge $\mathbb{Z}_n = \{0, 1, \ldots, (n-1)\}$ der Reste modulo n erfolgt.

Beispiel.

$$\begin{aligned} -16 \bmod 5 &= -16 - 5\lfloor -16/5 \rfloor = -16 - 5\lfloor -3.2 \rfloor = -16 - 5(-4) = -16 + 20 = 4 \\ &= 9 \bmod 5 = 9 - 5\lfloor 9/5 \rfloor = 9 - 5(1) = 4 \end{aligned}$$

-16 hat den gleichen Rest bei Division mit 5 wie 9, daher gilt

$$9 \equiv -16 \pmod{5}$$

Bei gleichen Resten heben sich diese bei der Subtraktion von x und y weg und für $x - y$ ergibt sich ein Vielfaches von n, $x - y$ ist also durch n teilbar. Daraus folgt

$$x \equiv y \pmod{n} \quad \Longleftrightarrow \quad x - y \quad \text{ist ein Vielfaches von } n \text{ (teilbar durch } n). \tag{4}$$

Beispiel. Wegen $9 - (-16) = 25 = 5 \cdot 5$ gilt $9 \equiv -16 \pmod{5}$, da beide Seiten der Gleichung durch 5 teilbar sind (bzw. $9 - (-16)$ ein Vielfaches von 5 ist).

Wenn der Dividend x ein Vielfaches des Divisors n enthält, gilt

$$x = kn + m, \quad x, k \in \mathbb{Z},\ n \in \mathbb{N},\ 0 \leq m \leq (n-1), \quad (kn + m) \bmod n = m \bmod n \tag{5}$$

Beispiel.

$$15 \bmod 11 = (11 \cdot 1 + 4) \bmod 11 = 4 = -7 \bmod 11 = (11 \cdot 1 - 7) \bmod 11 = 4 \bmod 11 = 4$$

Der modulo n Operator bildet folglich alle ganzen Zahlen $\mathbb{Z}$ nach $\mathbb{Z}_n$ ab. Innerhalb dieser Menge gelten die Regeln der allgemeinen Arithmetik für die Addition, Subtraktion und Multiplikation.

Wenn $m \in \mathbb{Z}_n$ und $\gcd(m, n) = 1$, dann hat m eine eindeutige multiplikative Inverse in $\mathbb{Z}_n$, für die m^{-1} geschrieben wird.

$$\gcd(m, n) = 1, \text{ dann gibt es für } m \in \mathbb{Z}_n \text{ ein } b \text{ mit } mb \equiv 1 \pmod{n} \text{ und } b = m^{-1}. \tag{6}$$

Beweis. Da $\gcd(m, n) = 1$ ist, kann 1 als Linearkombination von m und n ausgedrückt werden. Das heißt, daß es ganze Zahlen r und t gibt, für die $1 = rm+nt$ bzw. $1-rm = nt$ und somit $1 \equiv rm \pmod{n}$. Dies gilt dann und nur dann, wenn m teilerfremd zu n ist. Ist $n = p$ eine Primzahl, so hat jedes Element außer 0 aus $\mathbb{Z}_n$ eine multiplikative Inverse. $\square$

Beispiel. Für die multiplikativen und additiven Inversen modulo 7 folgt:

m	$-m$	m^{-1}
0	0	–
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Für $m = 2$ gilt z.B. $2 \cdot 4 \bmod 7 = 1 \bmod 7$ und damit $2^{-1} = 4$. Außerdem gilt $(2 + 5) \bmod 7 = 0 \bmod 7$. Die additive Inverse von 2 modulo 7 ist also $-2 = 5$.

$$\text{Für jedes } m \in \mathbb{Z}_n \text{ gibt es ein } b \text{ mit } m + b \equiv 0 \pmod{n}, \text{ geschrieben } b = -m. \tag{7}$$

Beispiel. In $\mathbb{Z}_{26}$ gibt es dagegen nur für folgende Zahlen multiplikative Inverse: $1^{-1} = 1$, $3^{-1} = 9$, $5^{-1} = 21$, $7^{-1} = 15$, $11^{-1} = 19$, $17^{-1} = 23$ und $25^{-1} = 25$. Es gilt z.B. $7 \cdot 15 = 105 \equiv 1 \pmod{26}$ und daher $7^{-1} = 15$.

Bevor ich nun einige Rechenregeln der modularen Arithmetik anführe, möchte ich zuerst etwas zur Nomenklatur sagen. Diese ist leider nicht in allen Büchern einheitlich, oft wird sogar in ein und demselben Buch die Schreibweise nach belieben geändert. In [6] wird z.B. überall „=“ verwendet. Gleichung (3) wird so zu $x = y \pmod{n}$ und für den unbedarften Leser fängt das Chaos an. In [2] wird einmal „=“ und ein anderes Mal „≡“ verwendet, vermutlich je nachdem, welche Quelle der Autor verwendet hat. Ein Versuch, ihn darauf hinzuweisen, stoß auf Unverständnis. Eine gewisse Vorsicht ist auch bei der Verwendung von „≡“ geboten (siehe z.B. [7]), da z.B. für die Äquivalenzrelation mitunter das gleiche Symbol (neben „$\Longleftrightarrow$“) verwendet wird.

Und nun zu den Rechenregeln.

Satz 6. Es gilt $n \in \mathbb{N}$ und $w, x, y, z \in \mathbb{Z}$.

1. $x \equiv x \pmod{n}$
2. $x \equiv y \pmod{n}$ impliziert $y \equiv x \pmod{n}$

3. $x \equiv y \pmod{n}$ und $y \equiv z \pmod{n}$ impliziert $x \equiv z \pmod{n}$ (Transitivität)
4. $x \equiv y \pmod{n}$ und $w \equiv z \pmod{n}$ impliziert $x + w \equiv y + z \pmod{n}$ und $xw \equiv yz \pmod{n}$
5. $x \equiv y \pmod{n}$ impliziert $xz \equiv yz \pmod{n}$
6. $x \equiv y \pmod{n}$ impliziert $x^k \equiv y^k \pmod{n}$ für $k \in \mathbb{N}$
7. $\big[(x \bmod n) \pm (y \bmod n)\big] \bmod n = (x \pm y) \bmod n$
8. $\big[(x \bmod n)(y \bmod n)\big] \bmod n = (xy) \bmod n$

Beweis. Exemplarisch sollen die Regeln 3, 4, 6 und 8 bewiesen werden.

Zuerst Regel 3. Wegen (4) gibt es zwei ganze Zahlen r, s mit $x - y = rn$ und $y - z = sn$. Addiert man die beiden Gleichungen, so erhält man $x - z = (r + s)n$, woraus $x \equiv z \pmod{n}$ folgt.

Für Regel 4 gilt analog $x - y = rn$ und $w - z = sn$ mit $r, s \in \mathbb{Z}$. Durch Addition der beiden Gleichungen erhält man $(x + w) - (y + z) = (r + s)n$ und damit $x + w \equiv y + z \pmod{n}$.

Der zweite Teil von Regel 4 besagt, daß $xw \equiv yz \pmod{n}$. Mit (4) und $r \in \mathbb{Z}$ folgt $xw - yz = rn$. Durch Erweiterung der linken Seite der Gleichung mit $yw - yw = 0$ erhält man $xw - yw + yw - yz = rn = (x - y)w + y(w - z)$. Da n, wie oben gezeigt, $x - y$ und $w - z$ teilt, ist der zweite Teil der Regel bewiesen.

Der Beweis des zweiten Teils von Regel 4 kann zum Beweis von Regel 6 verwendet werden. Dazu ist $w = x$ und $z = y$ zu setzen. Dann gilt mit $r \in \mathbb{Z}$ und der Erweiterung von oben $x^2 - y^2 = (x - y)x + y(x - y) = rn$ und damit $x^2 \equiv y^2 \pmod{n}$. Für $w = x^2$ und $z = y^2$ folgt analog $x^3 - y^3 = (x - y)x^2 + y(x^2 - y^2)$. Setzt man nun das Ergebnis aus dem vorhergehenden Schritt, $x^2 - y^2 = (x - y)x + y(x - y)$ in die Gleichung ein, so erhält man $x^3 - y^3 = (x - y)x^2 + y(x - y)x + y^2(x - y)$ und damit $x^3 \equiv y^3 \pmod{n}$. Fährt man mit diesem Verfahren fort, so erhält man $x^k \equiv y^k \pmod{n}$.

Für Regel 8 wird zuerst $x \bmod n = r_x$ und $y \bmod n = r_y$ gesetzt. Mit (1) folgt dann $x = jn + r_x$ und $y = kn + r_y$ für beliebige $j, k \in \mathbb{Z}$. Daraus folgt

$$\begin{aligned}
\big[(x \bmod n)(y \bmod n)\big] \bmod n &= \big[(x - jn)(y - kn)\big] \bmod n \\
&= \big[xy - xkn - jny + jknn\big] \bmod n, \quad \text{und wegen (5)} \\
&= (xy) \bmod n
\end{aligned}$$

$\square$

Mehr Zahlentheorie

Eine weitere wichtige Größe der Zahlentheorie ist die eulersche Funktion ϕ (im Englischen auch *totient function* genannt).

Definition 5. Die Funktion $\phi(n)$ ist die Anzahl ganzer positiver Zahlen, die kleiner als n und zu n teilerfremd sind.

Beispiel. $\phi(7) = 6$, da es sechs ganze positive Zahlen ($M = \{1, 2, 3, 4, 5, 6\}$) gibt, für die $\gcd(x, 7) = 1$, $x \in M$, ist.

$\phi(6) = 2$, da es nur zwei ganze positive Zahlen gibt, die zu 6 teilerfremd sind, nämlich 1 und 5.

$\phi(16) = 8$, da $1, 3, 5, 7, 9, 11, 13$ und 15 die einzigen ganzen positiven Zahlen sind, die kleiner als 16 und zu 16 teilerfremd sind.

Für $\phi(n)$ gibt es einige Rechenregeln, die im folgenden hergeleitet und bewiesen werden.

Satz 7. Ist p eine Primzahl, so gilt $\phi(p) = p - 1$.

Beweis. Die einzigen Teiler von p sind p und 1. Daher sind alle ganzen positiven Zahlen kleiner p (nämlich, $1, 2, \ldots, p - 1$) zu p teilerfremd. $\square$

Satz 8. Sind p und q unterschiedliche Primzahlen, so gilt $\phi(pq) = (p - 1)(q - 1) = \phi(p)\phi(q)$.

Beweis. Es gibt $pq-1$ ganze Zahlen kleiner pq. Davon sind die Zahlen $p, 2p, 3p, \ldots, (q-1)p$ durch p teilbar und $q, 2q, 3q, \ldots, (p - 1)q$ durch q. Es bleiben also $pq - 1 - (q - 1) - (p - 1) = pq - p - q + 1 = (p - 1)(q - 1)$ Zahlen übrig, die weder durch p noch durch q geteilt werden können und daher mit pq teilerfremd sind. $\square$

Beispiel. $\phi(3 \cdot 5) = \phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$, nämlich $1, 2, 4, 7, 8, 11, 13, 14$.

Satz 9. Falls p eine Primzahl und k eine ganze positive Zahl ist, so gilt $\gcd(n, p^k) = 1$ dann und nur dann, wenn p nicht n teilt.

Beweis. Sollte $p|n$, so wäre $\gcd(n, p^k) \neq 1$, da p auch p^k teilt. Umgekehrt, wenn $\gcd(n, p^k) \neq 1$, dann sind n und p^k nicht teilerfremd und sie müssen einen gemeinsamen Faktor größer 1 haben. Da aber die einzigen Faktoren von p^k Potenzen von p sind, gilt $p|n$. $\square$

Satz 10. Ist p eine Primzahl und k eine positive ganze Zahl, so gilt $\phi(p^k) = p^k - p^{k-1}$.

Beweis. Von 1 bis p^k gibt es p^{k-1} ganze Zahlen $(p, 2p, 3p, \ldots, p^{k-1}p^k)$, die durch p teilbar sind. Dazu gehört auch p^k selbst. Es bleiben also $p^k - p^{k-1}$ Zahlen übrig, die positiv und kleiner als p^k sind. □

Beispiel. Für $p = 2$ und $k = 3$ folgt $p^k = 2^3 = 8$ mit $\phi(8) = 4$. Das gleiche Ergebnis erhält man mit $p^k - p^{k-1} = 2^3 - 2^2 = 4$.

Satz 11. Für ganze Zahlen a, b und c gilt $\gcd(a, bc) = 1$ dann und nur dann, wenn auch $\gcd(a, b) = 1$ und $\gcd(a, c) = 1$.

Beweis. Angenommen, $\gcd(a, bc) = 1$. Es ist zu zeigen, daß $\gcd(a, b) = 1$. Angenommen, $\gcd(a, b) = d$. Dann gilt $d|a$ und $d|b$. Da aber $\gcd(a, bc) = 1$ ist, muß $d = 1$, nämlich der größte gemeinsame Teiler von a und bc, sein. Die gleiche Argumentation gilt für $\gcd(a, c) = 1$.

Umgekehrt sei angenommen, daß $\gcd(a, b) = 1$ und $\gcd(a, c) = 1$. Es ist zu zeigen, daß $\gcd(a, bc) = 1$. Angenommen, $\gcd(a, bc) = d > 1$. Dann muß d eine Primzahl p enthalten, die $p|a$ und $p|bc$. Also gilt $p|b$ oder $p|c$. Wenn aber $p|b$ und $p|a$ so muß wegen $\gcd(a, b) = 1$ auch $p|1$ und kann daher keine Primzahl sein. Wenn andererseits $p|c$ und $p|a$, so muß wegen $\gcd(a, c) = 1$ wiederum $p|1$, was ausschließt, daß p eine Primzahl ist. Die Annahme $\gcd(a, bc) > 1$ führt also zu einem Widerspruch und es ist daher $\gcd(a, bc) = 1$. □

Beispiel. Angenommen $a = 5$, $b = 6$ und $c = 7$. Dann ist $\gcd(5, 6) = 1 = \gcd(5, 7)$. Es muß also auch $\gcd(5, 6 \cdot 7) = \gcd(5, 42) = 1$ sein.

Ist andererseits $a = 5$, $b = 6$ und $c = 15$, so folgt $\gcd(5, 6) = 1$ aber $\gcd(5, 15) = 5$ und damit $\gcd(5, 90) = 5 \neq 1$.

Jetzt wird es noch spannender.

Satz 12. Wenn m und n teilerfremde positive ganze Zahlen sind, so gilt $\phi(mn) = \phi(m)\phi(n)$.

Beweis. Die Zahlen von 1 bis mn sind $1, 2, \ldots, r, \ldots, mn$. Ordnet man diese Zahlen in einer $n \times m$-Matrix mit n Zeilen und m Spalten an, so erhält man

$$\begin{array}{cccccc}
1 & 2 & \ldots & r & \ldots & m \\
m+1 & m+2 & \ldots & m+r & \ldots & 2m \\
2m+1 & 2m+2 & \ldots & 2m+r & \ldots & 3m \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+r & \ldots & nm
\end{array}$$

$\phi(mn)$ ist die Anzahl der Elemente a_{ij}, $1 \le i \le n$, $1 \le j \le m$, die teilerfremd zu mn sind, für die also $\gcd(a_{ij}, mn) = 1$ gilt. Laut Satz 11 muß dann aber auch $\gcd(a_{ij}, m) = 1$ und $\gcd(a_{ij}, n) = 1$ erfüllt sein.

Wenn d die kleinste ganze Zahl ist, die als Linearkombination von $qm + r$ und m ausgedrückt werden kann, $d = a(qm + r) + bm$, $a, b \in \mathbb{Z}$, so ist d auch die kleinste ganze Zahl, die eine Linearkombination von m und r, $d = (aq + b)m + ar$, ist. Es gilt also $\gcd(qm+r, m) = \gcd(r, m)$. Das heißt aber, daß die Zahlen in der r-ten Spalte nur dann teilerfremd zu m sind, wenn r selbst es ist. Es gibt also $\phi(m)$ Spalten, die teilerfremd zu m sind und jede Zahl in diesen Spalten ist es ebenfalls.

Es ist als noch zu zeigen, daß in jeder der $\phi(m)$ Spalten $\phi(n)$ Elemente teilerfremd zu n sind. Nur dann sind $\phi(m)\phi(n)$ Elemente teilerfremd zu beiden, m und n.

Angenommen, $\gcd(r, m) = 1$. Es sollen dann die Elemente der r-ten Spalte, $r, m + r, 2m + r, \dots, (n - 1)m + r$ auf Teilerfremdheit zu n untersucht werden. Die Spalte hat n Elemente, wobei keine zwei kongruent modulo n zueinander sind. Falls sie es wären, müßte nämlich $km + r \equiv jm + r \pmod{n}$ bzw. $km \equiv jm \pmod{n}$, $0 \le j < k < n$, sein. Das heißt, es gäbe eine ganze Zahl t, für die $km - jm = tn$ bzw. $m(k - j) = tn$. Da $n|tn$ muß auch $n|m(k - j)$. Es ist aber $\gcd(m, n) = 1$ und so kann nur $n|(k - j)$ woraus $k - j = un$, $u \in \mathbb{Z}$, folgt. Dies heißt aber, daß $k \equiv j \pmod{n}$, was aber ein Widerspruch ist, da aus $0 \le j < k < n$ auch $k - j < n$ folgt und n daher nicht $k - j$ teilen kann.

Die Zahlen a_{ir}, $1 \le i \le n$, in der r-ten Spalte sind folglich in irgendeiner Reihenfolge kongruent modulo n zu den Elementen von $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$. Für $s \in \mathbb{Z}_n$ und $s \equiv a_{ir} \pmod{n}$ gilt $\gcd(a_{ir}, n) = 1$ dann und nur dann, wenn auch $\gcd(s, n) = 1$ ist. Denn es folgt aus $\gcd(s, n) = 1$, daß es zwei ganze Zahlen a, b gibt, für die $as + bn = 1$. Für $\nu \in \mathbb{Z}$ folgt aus $s \equiv a_{ir} \pmod{n}$ aber $s - a_{ir} = \nu n$ und damit $a(a_{ir} + \nu n) + bn = aa_{ir} + (a\nu + b)n = 1$, woraus wiederum $\gcd(a_{ir}, n) = 1$ folgt.

Die r-te Spalte enthält also soviele ganze Zahlen, die teilerfremd zu n sind, wie sie die Menge $\mathbb{Z}_n$ enthält, nämlich $\phi(n)$. Daher ist die Gesamtzahl ganzer Zahlen, die teilerfremd zu m und n sind, $\phi(m)\phi(n)$. □

Beispiel.

$$
\begin{aligned}
&m = 3,\ n = 4, \quad \phi(3)\phi(4) = 2 \cdot 2 = 4 = \phi(12) = \phi(3 \cdot 4)\\
&m = 7,\ n = 2, \quad \phi(7)\phi(2) = 6 \cdot 1 = 6 = \phi(14) = \phi(7 \cdot 2)\\
&m = 4,\ n = 2, \quad \phi(4)\phi(2) = 2 \cdot 1 = 2 \neq \phi(4 \cdot 2) = \phi(8) = 4, \text{ da } \gcd(4, 2) = 2 \neq 1
\end{aligned}
$$

Satz 12 kann auf ein Produkt von Primzahlen erweitert werden.

Satz 13. Wenn es für $n > 1$ die Primzahlzerlegung $n = p_1^{k_1} \cdot p_2^{k_2} \dots p_r^{k_r}$ gibt, so ist $\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$.

Beweis. Der Beweis erfolgt mit vollständiger Induktion. Der Induktionsbeginn für $r = 1$ ist wegen Satz 10 erfüllt.

Angenommen, die Beziehung gilt für $r = m$. Das heißt, wenn $n = p_1^{k_1} \cdot p_2^{k_2} \dots p_m^{k_m}$ folgt $\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_m^{k_m} - p_m^{k_m-1})$.

Für $r = m + 1$ ist dann $n = \left(p_1^{k_1} \cdot p_2^{k_2} \dots p_m^{k_m}\right) p_{m+1}^{k_{m+1}}$ und mit Satz 12 folgt $\phi(n) = \phi(p_1^{k_1} \cdot p_2^{k_2} \dots p_m^{k_m})\phi(p_{m+1}^{k_{m+1}})$. Satz 10 ergibt zusammen mit der Induktionsvoraussetzung $\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_{m+1}^{k_{m+1}} - p_{m+1}^{k_{m+1}-1})$. □

Mit Hilfe von Satz 13 kann $\phi(n)$ auch für große n relativ einfach bestimmt werden.

Beispiel.

$$\phi(360) = \phi(2^3 \cdot 3^2 \cdot 5) = (2^3 - 2^2)(3^2 - 3^1)(5^1 - 5^0) = 4 \cdot 6 \cdot 4 = 96$$
$$\phi(1575) = \phi(3^2 \cdot 5^2 \cdot 7) = (3^2 - 3^1)(5^2 - 5^1)(7^1 - 7^0) = 6 \cdot 20 \cdot 6 = 720$$

Satz 14. Für $n > 2$ ist $\phi(n)$ eine gerade Zahl.

Beweis. Wenn n eine Zweierpotenz ist, $n = 2^k$, $k > 1$, dann folgt aus Satz 10 $\phi(n) = \phi(2^k) = 2^k - 2^{k-1} = 2^{k-1}(2-1) = 2^{k-1}$, was eine gerade Zahl ist.

Ist n keine Zweierpotenz, so muß n durch eine ungerade Primzahl p teilbar sein, $n = p^k m$, $k \geq 1$. Dann gilt $\gcd(p^k, m) = 1$ und damit $\phi(n) = \phi(p^k m) = (p^k - p^{k-1})\phi(m) = p^{k-1}(p-1)\phi(m)$. Dies ist aber eine gerade Zahl, da $2|(p-1)$. □

Satz 15. Es sei $n > 1$ und $\gcd(a, n) = 1$. Wenn $a_1, a_2, \dots, a_{\phi(n)}$ die positiven ganzen Zahlen kleiner n und teilerfremd zu n sind, so sind die Zahlen $aa_1, aa_2, \dots, aa_{\phi(n)}$ kongruent modulo n zu $a_1, a_2, \dots, a_{\phi(n)}$ in irgendeiner Reihenfolge.

Beweis. Zuerst ist festzustellen, daß keine zwei Zahlen aus $\{aa_1, aa_2, \dots, aa_{\phi(n)}\}$ kongruent modulo n zueinander sind. Wäre dem nicht so, so würde $aa_i \equiv aa_j \pmod n$ für $i \neq j$ sein und damit $aa_i - aa_j = a(a_i - a_j) = kn$ für $k \in \mathbb{Z}$. Da aber $n|kn$, muß auch $n|a(a_i - a_j)$. Wegen $\gcd(a, n) = 1$ kann aber nur $n|(a_i - a_j)$, woraus $a_i - a_j = tn$, $t \in \mathbb{Z}$ und damit $a_i \equiv a_j \pmod n$ folgt. Dies ist aber ein Widerspruch, da $1 \leq a_j < a_i < n$ und damit $a_i - a_j < n$, woraus folgt, daß n nicht $a_i - a_j$ teilen kann. Eine ähnliche Schlußfolgerung führte schon in Satz 12 zum Ziel.

Da $\gcd(a, n) = 1 = \gcd(a_1, n) = \gcd(a_2, n) = \cdots = \gcd(a_{\phi(n)}, n)$ ist, garantiert Satz 11 ferner $\gcd(aa_1, n) = \gcd(aa_2, n) = \cdots = \gcd(aa_{\phi(n)}, n) = 1$.

Angenommen, es gilt $aa_i \equiv b \pmod n$ für irgendein $b \in \mathbb{Z}_n$ und damit $aa_i - b = kn$, $k \in \mathbb{Z}$. Damit ist $1 = \gcd(aa_i, n) = \gcd(b, n)$, weil für ganze Zahlen x, y die Linearkombination $1 = x(aa_i) + yn = x(b + kn) + yn = xb + (kx + y)n$ ist. Damit muß aber b eine der Zahlen $a_1, a_2, \ldots, a_{\phi(n)}$ sein, weil dies die einzigen Zahlen sind, die teilerfremd zu n sind. Daher ist $aa_i \equiv b \pmod{n}$ mit $b \in \{a_1, a_2, \ldots, a_{\phi(n)}\}$. □

Beispiel. Es sei $n = 8$ und $a = 5$ und damit $\gcd(5, 8) = 1$. Alle positiven ganzen Zahlen kleiner 8 und teilerfremd zu 8 sind $S = \{1, 3, 5, 7\}$. Multipliziert man nun jedes Element von S mit 5, so erhält man $R = \{5, 15, 25, 35\}$. Satz 15 besagt, daß jedes Element aus R kongruent modulo 8 zu einem Element aus S sein muß. Dies trifft tatsächlich zu, da $5 \equiv 5 \pmod{8}$, $15 \equiv 7 \pmod{8}$, $25 \equiv 1 \pmod{8}$ und $35 \equiv 3 \pmod{8}$.

Es ist geschafft. Nun zu dem Satz, der diesen ganzen Aufwand rechtfertigt, zum **Satz von Euler**.

Satz 16. Wenn n eine ganze positive Zahl ist, mit $\gcd(a, n) = 1$, dann gilt

$$a^{\phi(n)} \equiv 1 \pmod{n}. \tag{8}$$

Beweis. Der Satz gilt für $n = 1$, da mit $\phi(1) = 0$ unmittelbar $a^0 \equiv 1 \pmod{1}$ folgt. Es ist zu erwähnen, daß für $\phi(1)$ nicht überall Null gesetzt wird, wie dies z.B. in [2] oder [7] der Fall ist. In [1] wird $\phi(1) = 1$ gesetzt und in [5] ist $\phi(n)$ nur für $n \geq 2$ definiert. Dies tut aber der Gültigkeit von (8) keinen Abbruch, da auch $a^1 \equiv 1 \pmod{1}$ für $k \in \mathbb{Z}$ wegen $a - 1 = k$ erfüllt ist, nämlich für $k = a - 1$.

Für $n > 1$ sind $a_1, a_2, \ldots, a_{\phi(n)}$ die positiven ganzen Zahlen kleiner n, die teilerfremd zu n sind.

$\gcd(a, n) = 1$ vorausgesetzt, besagt Satz 15, daß die Werte $aa_1, aa_2, \ldots, aa_{\phi(n)}$ in irgendeiner Reihenfolge kongruent modulo n zu $a_1, a_2, \ldots, a_{\phi(n)}$ sind. Das heißt,

$$\begin{aligned} aa_1 &\equiv a'_1 \pmod{n} \\ aa_2 &\equiv a'_2 \pmod{n} \\ &\vdots \\ aa_{\phi(n)} &\equiv a'_{\phi(n)} \pmod{n} \end{aligned}$$

Wegen Satz 6, Regel 4, können die Terme links und rechts der Äquivalenz miteinander multipliziert werden. Daraus folgt

$$\begin{aligned} aa_1 aa_2 \cdots aa_{\phi(n)} &\equiv a'_1 a'_2 \cdots a'_{\phi(n)} \pmod{n} \quad \text{bzw.} \\ aa_1 aa_2 \cdots aa_{\phi(n)} &\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \end{aligned}$$

und damit

$$a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}$$

Setzt man $x = a_1 a_2 \cdots a_{\phi(n)}$ so folgt $a^{\phi(n)} x \equiv x \pmod{n}$ und wegen Satz 11 auf Seite 13 $\gcd(x, n) = 1$.

Damit ist $a^{\phi(n)} x - x = kn$ bzw. $x(a^{\phi(n)} - 1) = kn$ für $k \in \mathbb{Z}$. Da $n | kn$ muß auch $n | x a^{\phi(n)}$. Weil aber $\gcd(n, x) = 1$ kann nur $n | (a^{\phi(n)} - 1)$ und damit $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Beispiel. Für $a = 5$, $n = 8$ ist $\gcd(5, 8) = 1$ und $\phi(8) = 4$ bzw. $5^{\phi(8)} = 5^4 = 625$. Somit ist $625 \equiv 1 \pmod{8}$ weil $625 - 1 = 624 = 8 \cdot 78$.

Für $a = 2$, $n = 7$ ist $\gcd(2, 7) = 1$ und $\phi(7) = 6$ bzw. $2^{\phi(7)} = 2^6 = 64$. Somit ist $64 \equiv 1 \pmod{7}$ weil $64 - 1 = 63 = 9 \cdot 7$.

Ist p eine Primzahl, die a nicht teilt, $\gcd(a, p) = 1$, gilt der Satz von Euler und es folgt $a^{\phi(p)} \equiv 1 \pmod{p}$. Wegen Satz 7 gilt dann $a^{p-1} \equiv 1 \pmod{p}$. Da dies Ergebnis unabhängig von Euler 1640 von Fermat entdeckt wurde, wird es **Satz von Fermat** (manchmal auch der kleine Satz von Fermat) genannt.

Satz 17. Ist p eine Primzahl mit $\gcd(a, p) = 1$, so gilt

$$a^{p-1} \equiv 1 \pmod{p}. \tag{9}$$

Beispiel. Ist $p = 5$ und $a = 2$, so folgt $a^{\phi(p)} = 2^4 = 16 \equiv 1 \pmod{5}$.

Ist n das Produkt zweier Primzahlen, so führt Satz 8 zu folgendem **Zusatz zum Satz von Euler**:

Satz 18. Ist a teilerfremd zu den beiden unterschiedlichen Primzahlen p und q, so gilt

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}. \tag{10}$$

Beispiel. Sei $p = 13$, $q = 113$ und $a = 939$. Da $a = 939 = 3 \cdot 313$ ist, ist es teilerfremd zu den beiden Primzahlen 13 und 113 und es gilt $939^{12 \cdot 112} = 939^{1344} \equiv 1 \pmod{1469}$.

Der RSA-Algorithmus

Alle Berechnungen des RSA-Algorithmus finden in der Menge $\mathbb{Z}_n$ statt, wobei $n = pq$ ist und p, q unterschiedliche große Primzahlen. Für die eulersche Funktion gilt dann $\phi(n) = (p - 1)(q - 1)$.

Satz 19. Es sei $m < n$ die zu verschlüsselnde Nachricht, $n = pq$, p, q unterschiedliche Primzahlen. Der öffentliche Schlüssel sei e, $1 < e < \phi(n)$ mit $\gcd(e, \phi(n)) = 1$, der private d, mit $ed \equiv 1 \pmod{\phi(n)}$ bzw. $d \equiv e^{-1} \pmod{\phi(n)}$. Wenn $c = m^e \bmod n$ und $m' = c^d \bmod n$ dann $m' = m$.

Beweis. Es ist $m' = c^d \bmod n = (m^e \bmod n)^d \bmod n$ und wegen Satz 6, Regel 8, $m' = m^{ed} \bmod n$. Wenn gezeigt werden kann, daß $m^{ed} \equiv m \pmod{n}$, dann ist $m' = m$.

Zuerst soll gezeigt werden, daß $m^{ed} \equiv m \pmod{p}$. Wegen $ed \equiv 1 \pmod{\phi(n)}$ gibt es eine ganze Zahl t mit $ed - 1 = t\phi(n)$ bzw. $ed = 1 + t\phi(n) = 1 + t(p-1)(q-1)$.

Im Fall, daß m und p nicht teilerfremd sind $(p|m)$, ist $m \equiv 0 \pmod{p}$ und $m^{ed} \equiv 0 \pmod{p}$ und damit wegen Satz 6, Regel 3, $m^{ed} \equiv m \pmod{p}$.

Sind m und p teilerfremd ($\gcd(m,p) = 1$), gilt

$$\begin{aligned} m^{ed} \bmod p &= m^{1+t(p-1)(q-1)} \bmod p \\ &= m \cdot m^{t(p-1)(q-1)} \bmod p \\ &= m(m^{p-1})^{t(q-1)} \bmod p \\ &= m(m^{\phi(p)})^{t(q-1)} \bmod p \end{aligned}$$

und mit Satz 6, Regel 8,

$$= \Big\{(m \bmod p)\big[(m^{\phi(p)})^{t(q-1)} \bmod p\big]\Big\} \bmod p$$

sowie (8) und Satz 6, Regel 6 und 8,

$$\begin{aligned} &= \big[(m \bmod p)(1^{t(q-1)} \bmod p)\big] \bmod p \\ &= m \bmod p \end{aligned}$$

Die gleiche Schlußfolgerung ergibt $m^{ed} \equiv m \pmod{q}$.

Da aber $p|(m^{ed}-m)$ und $q|(m^{ed}-m)$ folgt, daß $pq|(m^{ed}-m)$, da p und q unterschiedliche Primzahlen sind. Es gibt also eine ganze Zahl r mit $m^{ed} - m = (pq)r = nr$ und damit ist $m \equiv m^{ed} \pmod{n}$. □

Beispiel. Da Bob und Alice wohl zu denen gehören, die ihren Nachrichtenverkehr verschlüsseln, sollen sie auch in diesem Beispiel auftreten. Bob wählt $p = 101$ und $q = 113$, woraus $n = pq = 11413$ und $\phi(n) = \phi(11413) = 100 \cdot 112 = 11200$ folgt. Um e zu erhalten, können z.B. alle Zahlen ermittelt werden, die $\phi(n)$ teilen. e wird dann aus den Zahlen gewählt, die nicht zu den Divisoren von $\phi(n)$ gehören. Da $11200 = 2^6 \cdot 5^2 \cdot 7$ ist, kann für e nur eine Zahl gewählt werden, die nicht durch 2, 5 oder 7 geteilt werden kann, also z.B. $e = 3533$. Für die multiplikative Inverse $e^{-1} = d$ erhält man dann (und nur dann) $d = 6597$, weil $3533 \cdot 6597 \equiv 1 \pmod{11200}$.

Bob hat also den öffentlichen Schlüssel $(3533, 11413)$ und den privaten $(6597, 11413)$.

Alice erhält den öffentlichen Schlüssel von Bob, entweder von ihm persönlich oder von einem authorisierten Schlüsselzentrum und verschlüsselt damit die Nachricht $m = 9726 < n = 11413$. Sie berechnet also $c = 9726^{3533} \bmod 11413 = 5761$ und schickt c an Bob.

Wenn Bob die Nachricht 5761 erhält, so dechiffriert er sie mit seinem privaten Schlüssel und erhält wieder $m = 5761^{6597} \bmod 11413 = 9726$.

Die Verschlüsselung und Entschlüsselung erscheint sehr rechenaufwendig. Es gibt aber effiziente Algorithmen, welche die Komplexität der Berechnung reduzieren können. Einige dieser Verfahren sind z.B. in [5] angeführt.

Die nachfolgende Abbildung 2 faßt den RSA-Algorithmus nochmals zusammen.

Erzeugung der Schlüssel

Erzeuge zwei große Primzahlen p, q

Berechne $n = pq$ und $\phi(n) = (p-1)(q-1)$

Wähle eine zufällige ganze Zahl e, $1 < e < \phi(n)$ mit $\gcd(e, \phi(n)) = 1$

Berechne d so, daß $ed \equiv 1 \pmod{\phi(n)}$

Öffentlicher Schlüssel: (e, n)

Privater Schlüssel: (d, n)

Chiffrierung

Nachricht: $m < n$

Chiffrierte Nachricht: $c = m^e \pmod{n}$

Dechiffrierung

Chiffrierte Nachricht: c

Nachricht: $m = c^d \pmod{n}$

Abbildung 2: Der RSA-Algorithmus

Literatur

[1] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison–Wesley Publishing Company, Reading, Massachusetts, USA, 1989. ISBN 0-201-55802-5.

[2] R. E. Lewand. *Cryptological Mathematics*. The Mathematical Association of America, Washington, DC, USA, 2000. ISBN 0-88385-719-7.

[3] W. Stallings. *Network and Internetworking Security*. Prentice–Hall, Englewood Cliffs, New Jersey, USA, 1995. ISBN 0-02-415483-0.

[4] W. Stallings. *Protect Your Privacy: The PGP User's Guide*. Prentice–Hall, Englewood Cliffs, New Jersey, USA, 1995. ISBN 0-13-185596-4.

[5] D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press, Boca Raton, Florida, USA, 1995. ISBN 0-8493-8521-0.

[6] J. C. A. van der Lubbe. *Basic Methods of Cryptography*. Cambridge University Press, Cambridge, UK, 2000. ISBN 0-521-55559-0.

[7] E. Weisstein. World of Mathematics, http://mathworld.wolfram.com/.

[8] P. R. Zimmermann. *Official PGP User's Guide*. MIT Press, 1995. ISBN 0-262-74017-6.