Aufgabenzettel 5.

5.1. Eulersche ϕ-Funktion.

(a) Zeige: Seien m, n natürliche Zahlen, so dass jeder Primteiler von m auch ein Primteiler von n ist. Dann ist $\phi(mn) = m\phi(n)$.

(b) Für welche Paare m, n natürlicher Zahlen gilt $\phi(mn) = \phi(n)$?

(c) Ist m ein Teiler von n, so ist $\phi(m)$ ein Teiler von $\phi(n)$.

(d) Zeige: Ist $(m, n) \neq 1$, so ist $\phi(mn) > \phi(m)\phi(n)$.

5.2. Verwende den Chinesischen Restsatz, um alle Zahlen a zu bestimmen, die Rest 1 oder 2 haben, wenn sie durch jede der Zahlen 3, 4 oder 5 geteilt werden. (Zum Beispiel ist $a = 17$ eine dieser Zahlen, denn $17 \equiv 2 \mod 3$, $17 \equiv 1 \mod 4$ und $17 \equiv 2 \mod 5$.).

5.3. RSA. (a) Alice verschlüsselt die Nachricht m mit dem öffentlichen Schlüssel $[51, 11]$. Der verschlüsselte Text sei 31. Bobs privater Schlüssel sei $[51, 3]$. Bestimme, falls möglich, den Klartext.

(b) Alice verschlüsselt die Nachricht m mit dem öffentlichen Schlüssel $[33, 7]$. Der verschlüsselte Text sei 9. Bobs privater Schlüssel sei ebenfalls $[33, 7]$. Bestimme, falls möglich, den Klartext.

Achtung: Man überprüfe jeweils, ob der private Schlüssel überhaupt zum öffentlichen Schlüssel passt!

5.4. Bitte wählen Sie eine Zahl $x \geq 500$ (nicht jeder die gleiche!) und betrachten Sie die Primzahlen p mit $p \leq x$. Dies sind mindestens 95 Primzahlen (für $x = 545$ sind es genau 100 Primzahlen). Sei $1 \leq k \leq 12$. Man bestimme für jede Restklasse $\overline{a}$ in $\mathbb{Z}/k$ die Anzahl $\pi(x)_{ak}$ der Primzahlen p mit $p \leq x$, die zu $\overline{a}$ gehören. Die Zahlen $\pi(x)_{ak}$ liefern eine Tabelle der folgenden Form (hier der Fall $x = 545$):

a \ k	1	2	3	4	5	$\cdots$	12
0	100	1	1	0	1	$\cdots$	0
1		99	47	?	24		?
2			52	?	?		?
3				52	?		
$\vdots$							$\vdots$
							?
11							26

Wo stehen Nullen, wo stehen Einsen? (Beweis!) Was kann man vermuten?

Präsenz-Aufgaben. Die Euler'sche ϕ-Funktion.

1. Berechne $\phi(n)$ für $n = 10,\ 100,\ 1000,\ 10000,\ 39,\ 162\,324$.

2. Wieviele Primitivwurzeln modulo p (Primzahl mit $30 \leq p \leq 50$) gibt es?

3. Zeige: Ist p eine Primzahl mit $p|n$, so gilt $(p-1)|\phi(n)$.

4. Die Zahl n habe t paarweise verschiedene ungerade Primfaktoren. Dann ist 2^t ein Teiler von $\phi(n)$.

5. Es gilt

$$\phi(2n) = \begin{cases} \phi(n) & \text{falls } n \text{ ungerade ist,} \\ 2\phi(n) & \text{falls } n \text{ gerade ist.} \end{cases}$$

6. Man rechnet leicht nach, dass die folgenden Gleichungen gelten:

$$\begin{aligned} \tfrac{3}{2}\phi(3) &= 1+2 \\ \tfrac{4}{2}\phi(4) &= 1+3 \\ \tfrac{5}{2}\phi(5) &= 1+2+3+4 \\ \tfrac{6}{2}\phi(6) &= 1+5 \\ \tfrac{7}{2}\phi(7) &= 1+2+3+4+5+6 \end{aligned}$$

Wie lautet die allgemeine Aussage? Man beweise sie. (Verify the assertions, make a general conjecture and prove the conjecture).

5.1. Euler's ϕ-funktion. (a) Let $m, n \in \mathbb{N}$ such that every prime divisor of m also divides n. Then $\phi(mn) = m\phi(n)$.

(b) Determine all pairs $m, n \in \mathbb{N}$ such that $\phi(mn) = \phi(n)$.

(c) If m divides n, then $\phi(m)$ divides $\phi(n)$.

(d) If $(m, n) \neq 1$, then $\phi(mn) > \phi(m)\phi(n)$.

5.2. Use the Chinese Remainder Theorem in order to determine all integers a such that a is congruent to 1 or 2, for $m = 3, 4, 5$. (For example, $a = 17$, since $17 \equiv 2 \mod 3,\ 17 \equiv 1 \mod 4$ und $17 \equiv 2 \mod 5$.).

5.3. RSA. (a) Alice encodes the message m with the public key $[51, 11]$, the encoded message is 31. The private key of Bob is $[51, 3]$. Decode, if possible.

(b) Alice encodes the message m with the public key $[33, 7]$, the encoded message is 9. The private key of Bob is also $[33, 7]$. Decode, if possible.

Note: First check, whether the private key and the public key fit together!

5.4. Choose your individual number $x \geq 500$ and look at the primes p with $p \leq x$. Let $1 \leq k \leq 12$. For each residue class $\overline{a}$ in $\mathbb{Z}/k$ determine the number $\pi(x)_{ak}$ of all primes $p \leq x$ which belong to $\overline{a}$. Above you see part of the table for the case $x = 545$. Question: Which entries are 0 or 1 (proof!), what may one conjecture?