Diophantische Gleichungen

A1:
Berechne mit dem Euklidischen Algorithmus:
a. ggT$(150, 54)$ b. ggT$(300, 468)$ c.ggT$(44, 18)$ d. ggT$(992, 999)$

A2:
Berechne den ggT der Zahlen a und b und stelle ihn in der Form $ax + by$ dar.
a. $a = 531, b = 93$ b. $a = 753, b = 64$

A3:
Bestimme - falls möglich - eine Lösung (x/y) der angegebenen Gleichung:
a. $96x + 66y = 6$ b.$96x + 66y = 18$
d. $119x + 143y = 4$ e. $91x + 35y = 12$.

A4:
Vereinfache die Gleichung und finde möglichst viele Lösungen:
a. $42x + 126y = 84$ b. $81x + 54y = 27$ c. $77x + 121y = 44$

Kongruenzen

A5:
Bestimme möglichst alle ganzzahligen Lösungen x der folgenden Gleichungen:
a. $5 + x \equiv 2 \mod 7$ b. $5 \cdot x \equiv 2 \mod 7$
c. $5 \cdot x \equiv 2 \mod 10$ d. $-34 \equiv x \mod 5$

A6:
Beweise die folgenden Aussagen:
a. Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann $a + c \equiv b + d \mod m$.
b. Wenn $a \equiv b \mod m$, dann $-a \equiv -b \mod m$.
c. Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann $a \equiv c \mod m$.

Restklassen

A7:
Bestimme mit dem erweiterten Euklidschen Algorithmus:
a. $\frac{\overline{5}}{\overline{33}}$ in $\mathbb{Z}_{37}$. b. $\frac{\overline{7}}{\overline{20}}$ in $\mathbb{Z}_{89}$.

A8:
Bestimme mit dem kleinen Satz von Fermat:
a. $\overline{4}^{-11}$ in $\mathbb{Z}_{13}$. b. $\overline{6}^{31}$ in $\mathbb{Z}_{29}$. c. $\overline{6}^{32}$ in $\mathbb{Z}_{29}$.

A9:
Berechne in $\mathbb{Z}_{23}$ die folgenden Brüche:
a. $\frac{\overline{1}}{\overline{5}^{21}}$ b. $\frac{\overline{1}}{\overline{10}^{13}}$ c. $\frac{\overline{7}}{\overline{10}^{12}}$ d. $\frac{\overline{7}}{\overline{22}}$

Diffie-Hellman

A10:
a. Alice und Bob vereinbaren die Primzahl p und die Primitivwurzel g. Alice wählt a, Bob wählt b. Welche Zahlen werden veröffentlicht und wie heißt der gemeinsame Schlüssel?
a. p = 7, g = 3, a = 3, b = 4. b. p = 23, g = 7, a = 15, b = 17.

A11:
Alice und Bob vereinbaren p = 11 und g = 2. Alice schicht an Bob A = 5 und Bob meldet an Alice B = 8. Da die Zahlen klein sind, kann die Diffie-Hellman Verschlüsselung geknackt werden. Wie heißt der Schlüssel K?

	1	2	3	4	5	6	7	8	9	10
2^x mod 11	2	4	8	5	10	9	7	3	6	1

RSA

A12:
Bob wählt p , q und Verschlüsselungsexponent e. Warum ist e ein zulässiger Verschlüsselungsexponent? Wie heißt der öffentliche, wie der private Schlüssel von Bob? Alice will an Bob die Nachricht n verschlüsselt übermitteln. Welche Zahl schickt sie an Bob? Wie entschlüsselt Bob die Nachricht?
a. p = 3, q = 11, e = 7, n = 6. b. p = 7, q = 11, e = 47, n = 2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	34	51	68	85	102	119	136	153	170	187	204	221	238	255
23	23	46	69	92	115	138	161	184	207	230	253	276	299	322	345
29	29	58	87	116	145	174	203	232	261	290	319	348	377	406	435
31	31	62	93	124	155	186	217	248	279	310	341	372	403	434	465
33	33	66	99	132	165	198	231	264	297	330	363	396	429	462	495
77	77	154	231	308	385	462	539	616	693	770	847	924	1001	1078	1155
91	91	182	273	364	455	546	637	728	819	910	1001	1092	1183	1274	1365

Quadratzahlen:
11-121 12-144 13-169 14-196 15-225 16-256 17-289 18-324 19-361 20-400 21-441 22-484 23-529 24-576 25-625 26-676 27-729 28-784 29-841 30-900