1. (2 Punkte) Berechne mit dem Euklidischen Algorithmus: $\mathrm{ggT}(88, 196)$

Lösung:

88	196
196	88
88	20
20	8
8	4
4	0

$\mathrm{ggT}(88, 196) = 4$

2. (3 Punkte) Berechne den ggT der Zahlen a und b und stelle ihn in der Form $ax + by$ dar: $a = 393, b = 87$

Lösung:

```
2 * 393  + -9 * 87 = 3
```

	a	b	q	r	x	y
0	393	87	4	45	2	-9
1	87	45	1	42	-1	2
2	45	42	1	3	1	-1
3	42	3	14	0	0	1

3. (3 Punkte) Bestimme - falls möglich - eine Lösung (x/y) der angegebenen Gleichung: $78x + 52y = 4$

Lösung:

```
1 * 78  + -1 * 52 = 26
```

	a	b	q	r	x	y
0	78	52	1	26	1	-1
1	52	26	2	0	0	1

Der ggT von 78 und 52 ist 26. 26 ist nicht Teiler von 4. Also hat die Gleichung keine Lösung.

4. (3 Punkte) Finde möglichst viele Lösungen für: $21x - 15y = 9$

Lösung:

$21x - 15y = 9 \quad | :3$

$7x - 5y = 3 \quad (1)$

Wir lösen zunächst:

$7x + 5y = 3 \quad (2)$

$(-1/2)$ ist Lösung für (2)

weitere Lösungen für (2): $(-1+5k / 2-7k)$

$(-1/-2)$ ist Lösung für (1)

weitere Lösungen für (1): $(-1+5k / -2+7k)$

5. (3 Punkte) Bestimme die ganzzahligen Lösungen x der folgenden Gleichung: $12 + 2x \equiv 3 \mod 7$

Lösung:

$$12 + 2x \equiv 3 \mod 7$$
$$2x \equiv -9 \equiv -2 \mod 7$$
$$x \equiv -1 \mod 7$$
$$\mathbb{L} = \{-1 + 7k \,;\, k \in \mathbb{Z}\}$$

6. (3 Punkte) Beweise die folgenden Aussage:
Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann $a + c \equiv b + d \mod m$.

Lösung:

$$\left.\begin{array}{l} a \equiv b \mod m \Rightarrow \exists k_1 \in \mathbb{Z}: \ a-b = k_1 \cdot m \\ c \equiv d \mod m \Rightarrow \exists k_2 \in \mathbb{Z}: \ c-d = k_2 \cdot m \end{array}\right\} (a-b)+(c-d) = k_1 \cdot m + k_2 \cdot m$$
$$(a+c)-(b+d) = \underbrace{(k_1+k_2)}_{\in \mathbb{Z}} \cdot m$$
$$\Rightarrow a+c \equiv b+d \mod m$$

7. (3 Punkte) Bestimme $\dfrac{\overline{8}}{\overline{17}}$ in $\mathbb{Z}_{41}$.

Lösung:

5 * 41 + -12 * 17 = 1

	a	b	q	r	x	y
0	41	17	2	7	5	-12
1	17	7	2	3	-2	5
2	7	3	2	1	1	-2
3	3	1	3	0	0	1

$$\frac{\overline{1}}{\overline{17}} = \overline{-12} \quad \text{in } \mathbb{Z}_{41}$$
$$\frac{\overline{8}}{\overline{17}} = \overline{8} \cdot (\overline{-12}) = \overline{-96} = \overline{27}$$

8. (3 Punkte) Bestimme $\overline{8}^{33}$ in $\mathbb{Z}_{29}$.

Lösung:

$$\overline{8}^{33} \equiv \overline{8}^{28+5} \equiv \overline{8}^{5} \equiv \underset{7 \cdot 8}{\overline{56}} \equiv \underline{\underline{\overline{27}}} \mod 29$$

$$\overline{8}^{1} \equiv \underline{8} \mod 29$$
$$\overline{8}^{2} \equiv 64 \equiv 6$$
$$\overline{8}^{4} \equiv 36 \equiv \underline{7}$$

9. (3 Punkte) (Diffie-Hellman) Alice und Bob vereinbaren die Primzahl p=11 und die Primitivwurzel g=6.
Alice wählt a=4, Bob wählt b=9. Welche Zahlen werden veröffentlicht und wie heißt der gemeinsame Schlüssel?

Lösung:

$$A \equiv 6^4 \mod 11$$
$$\equiv \underline{9}$$
$$B \equiv 6^9 \mod 11$$
$$\equiv 24 \equiv \underline{2}$$
$$K \equiv 2^4 \mod 11$$
$$\equiv 16 \equiv \underline{5}$$

$$6^1 \equiv 6 \mod 11$$
$$6^2 \equiv 36 \equiv 3$$
$$6^4 \equiv 9$$
$$6^8 \equiv 81 \equiv 4$$

Veröffentlicht werden die Zahlen p, g, A und B

10. (3 Punkte) (Diffie-Hellman) Alice und Bob vereinbaren $p = 17$ und $g = 10$. Alice veröffentlicht $A = 12$ und Bob veröffentlich $B = 8$. Wie heißen die Geheimnisse von Alice und Bob und der gemeinsame Schlüssel K?

Lösung:

$$12 = 10^a \mod 17 \Rightarrow \underline{a = 15}$$
$$8 = 10^b \mod 17 \Rightarrow \underline{b = 14}$$

$$\underline{K} = 8^{15} \mod 17$$
$$\equiv -8 \cdot 13 \equiv -104$$
$$\equiv -2 \equiv \underline{15}$$

$$8^1 \equiv 8 \mod 17$$
$$8^2 \equiv 64 \equiv 13$$
$$8^4 \equiv 169 \equiv -1$$
$$8^8 \equiv 1$$

Aufgabe:	1	2	3	4	5	6	7	8	9	10	Summe:
Punkte:	2	3	3	3	3	3	3	3	3	3	29

Hilfsmittel:

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

Die Potenzen von 10 mod 17

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
10^x mod 17	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1

Multiplikationsreihen

	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
29	29	58	87	116	145	174	203	232	261	290	319	348	377	406	435