Übungen zur Mathematik 1
Lösungen Kryptografie

Aufgabe 1

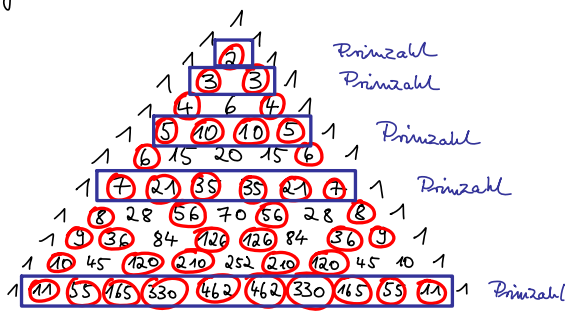
a) $8 \operatorname{div} 5 = 1$, $8 \bmod 4 = 0$, $25 \operatorname{div} 4 = 6$, $25 \bmod 4 = 1$,
$37 \operatorname{div} 11 = 3$, $37 \bmod 11 = 4$, $50 \operatorname{div} 7 = 7$, $50 \bmod 7 = 1$,
$1024 \operatorname{div} 23 = 44$, $1024 \bmod 23 = 12$,
$24536 \operatorname{div} 256 = 95$, $24536 \bmod 256 = 216$

b) $\mathbb{Z}_5$: $2+2=4$, $2+3=0$, $3+4=2$, $5+3=3$,
$11+25=1$, $20+30=0$, $2\cdot 2=4$, $2\cdot 3=1$,
$3\cdot 4=2$, $5\cdot 3=0$, $11\cdot 25=0$, $20\cdot 30=0$,
$2^3=3$, $4!=4$, $4^3=4$, $5^3=0$,
$11^{25}=1^{25}=1$, $20^{30}=0^{30}=0$.

$\mathbb{Z}_8$: $2+2=4$, $2+3=5$, $3+4=7$, $5+3=0$,
$11+25=2$, $20+30=2$, $2\cdot 2=4$, $2\cdot 3=6$,
$3\cdot 4=4$, $5\cdot 3=7$,
$11\cdot 25=3\cdot 1=3$,
$20\cdot 30=4\cdot 6=24=0$,
$2^3=0$, $4!=0$, $4^3=0$,
$5^3=25\cdot 5=1\cdot 5=5$,
$11^{25}=3^{25}=3^{24}\cdot 3=9^{12}\cdot 3=1^{12}\cdot 3=3$,
$20^{30}=4^{30}=16^{15}=0^{15}=0$.

$\mathbb{Z}_{11}$: $2+2=4$, $2+3=5$, $3+4=7$, $5+3=8$,
$11+25=0+3=3$, $20+30=6$,
$2\cdot 2=4$, $2\cdot 3=6$, $3\cdot 4=1$, $5\cdot 3=4$,
$11\cdot 25=0\cdot 3=0$, $20\cdot 30=9\cdot 8=6$,
$2^3=8$, $4!=2$, $4^3=16\cdot 4=5\cdot 4=9$,
$5^3=25\cdot 5=3\cdot 5=4$,
$11^{25}=0^{25}=0$,
$20^{30}=9^{30}=81^{15}=4^{15}=4\cdot(4^2)^7=4\cdot 5^7$
$=\underbrace{4\cdot 5}_{20}\cdot(25)^3=9\cdot 4^3=\underbrace{9\cdot 4}_{36}\cdot 16$
$=3\cdot 5=4$.

Aufgabe 2



Man sieht, dass für $n = 1, \dots, 12$ gilt:
Wenn n eine Primzahl ist, ist n Teiler von $\binom{n}{k}$ für $k = 1, \dots, n-1$.
Siehe Satz der Vorlesung:

$$p \text{ prim} \Rightarrow p \mid \binom{p}{k} \text{ für } k = 1, \dots, n-1.$$

Implikation gilt i. A. nicht, falls p keine Primzahl ist!

Aufgabe 3

Kleiner Fermatscher Satz: Sei p eine Primzahl. Dann gilt: $x^{p-1} = 1$ bzw. $x^p = x$ für alle $x \in \mathbb{Z}_p \setminus \{0\}$.
($x^{p-1} \bmod p = 1$, $x^p \bmod p = x$, $= \{1, \dots, p-1\}$)

	1	2	3	4	5	6
$x \bmod 7$	1	2	3	4	5	6
$x^2 \bmod 7$	1	4	2	2	4	1
$x^3 \bmod 7$	1	1	6	1	6	6
$x^4 \bmod 7$	1	2	4	4	2	1
$x^5 \bmod 7$	1	4	5	2	3	6
$x^6 \bmod 7$	1	1	1	1	1	1
$x^7 \bmod 7$	1	2	3	4	5	6

] kleiner Fermatscher Satz

	1	2	3	4	5	6	7	8	9	10
$x \bmod 11$	1	2	3	4	5	6	7	8	9	10
$x^2 \bmod 11$	1	4	9	5	3	3	5	9	4	1
$x^3 \bmod 11$	1	8	5	9	4	7	2	6	3	10
$x^4 \bmod 11$	1	5	4	3	9	9	3	4	5	1
$x^5 \bmod 11$	1	10	1	1	1	10	10	10	1	10
$x^6 \bmod 11$	1	9	3	4	5	5	4	3	9	1
$x^7 \bmod 11$	1	7	9	5	3	8	6	2	4	10
$x^8 \bmod 11$	1	3	5	9	4	4	9	5	3	1
$x^9 \bmod 11$	1	6	4	3	9	2	8	7	5	10
$x^{10} \bmod 11$	1	1	1	1	1	1	1	1	1	1
$x^{11} \bmod 11$	1	2	3	4	5	6	7	8	9	10

] kleiner Fermatscher Satz

Aufgabe 4

$4^7 = 4 \bmod 7$
$6^7 = 6 \bmod 7$
$9^{11} = 9 \bmod 11$
$8^{13} = 8 \bmod 13$
$5^{28} = 1 \bmod 29$
$27^{80} = 27 \cdot 27^{79} = \underbrace{27 \cdot 27}_{729} = 18 \bmod 79$

Aufgabe 5

a) Öffentlicher Schlüssel $(n,e) = (187,7)$.

Zu verschlüsselnder Text: HDM

ASCII-Zuordnung: 72, 68, 77

Verschlüsselung mittels

$$y = x^e \bmod n$$
$$= x^7 \bmod 187$$

H (72): $y = 72^7 \bmod 187$

$= 72 \cdot 72^2 \cdot 72^2 \cdot 72^2 \bmod 187$

$5184 = 135 \bmod 187$

$= 72 \cdot 135 \cdot 135 \cdot 135 \bmod 187$

$9720 = 183$, $18225 = 86 \bmod 187$

$= 183 \cdot 86 \bmod 187$

15738

$= \underline{30} \bmod 187$

114338

D (68): $y = 68^7 \bmod 187$

$= 68^3 \cdot 68^4 \bmod 187$

$= 85 \cdot 170 \bmod 187$

$= \underline{51} \bmod 187$

M (77): $y = 77^7 \bmod 187$

$= 77^3 \cdot 77^4 \bmod 187$

$= 66 \cdot 33 \bmod 187$

$= \underline{121}$

Verschlüsselte Nachricht: $\boxed{30, 51, 121}$

b) Geheimer Schlüssel $d = 23$

Zu entschlüsselnder Text: 30, 51, 121

Entschlüsselung mittels

$$x = y^{23} \bmod 187$$

$30^{23} = (30^6)^3 \cdot 30^5 \bmod 187$

$= (135)^3 \cdot 98 \bmod 187$

$= 16 \cdot 98 \bmod 187$

$= \underline{72} \bmod 187$

$51^{23} = (51^5)^4 \cdot 51^3 \bmod 187$

$= (153)^4 \cdot 68$

$= 34 \cdot 68$

$= \underline{68}$

20980

$121^{23} = (121^4)^5 \cdot 121^3 \bmod 187$

$= (33)^5 \cdot 110 \bmod 187$

$= 33 \cdot 110 \bmod 187$

$= \underline{77} \bmod 187$

Entschlüsselte Nachricht: 72, 68, 77

H D M

c) $n = 187 = \underbrace{11}_{p} \cdot \underbrace{17}_{q}$, $(p-1)(q-1) = 10 \cdot 16 = 160$

$e \cdot d = 7 \cdot 23 = 161 = 1 \bmod 160$