

Aufgabe 6

(a) $\Phi(28) = 12, \Phi(33) = 20, \Phi(35) = 24, \Phi(5^3) = 100$

Berechnet via (jeweils mit Parametern 28, 33, 35, 125)

```
perl -e 'sub euclid { $_[1] or return $_[0]; euclid ($_[1], $_[0] % $_[1]) }
$a = $ARGV[0]; euclid ($_, $a) == 1 and $s++ for 1..$a-1; print $s, "\n"'
```

- (b) \mathbb{P} sei die Menge der Primzahlen
 P_a sei die Menge der Primfaktoren von a
 T_a sei die Menge der Teiler von a

$$\begin{aligned}
 p \in \mathbb{P} &\stackrel{(1)}{\Rightarrow} P_{p^e} = \{p\} \\
 &\stackrel{(2)}{\Rightarrow} \forall n \in \{0, 1, 2, \dots, p^e\} : \text{ggT}(p^e, n) = 1, \text{ falls } p \nmid n \\
 &\Rightarrow \forall m \in M = \{0, 1, 2, \dots, p^{(e-1)}\} : (m \cdot p) \notin \mathbb{Z}_{p^e}^* \\
 &\Rightarrow \forall m \in M = \{n \cdot p \mid n \in \{0, 1, 2, \dots, p^{(e-1)}\}\} : m \notin \mathbb{Z}_{p^e}^* \wedge \\
 &\quad \forall i \in N = \{j \mid j \in \{0, 1, 2, \dots, p^e\} \wedge j \notin M\} : i \in \mathbb{Z}_{p^e}^* \wedge \\
 &\quad M \cup N = \mathbb{Z}_{p^e} \wedge M \cap N = \emptyset \\
 &\Rightarrow \Phi(p^e) \stackrel{(3)}{=} |\mathbb{Z}_{p^e}^*| \stackrel{(4)}{=} |\mathbb{Z}_{p^e}| - |M| = (p^e + 1) - (p^{(e-1)} + 1) \\
 &\quad = p^e + 1 - p^{(e-1)} - 1 = p^e - p^{(e-1)} = p \cdot p^{(e-1)} - p^{(e-1)} = (p-1)p^{(e-1)}
 \end{aligned}$$

- (1) folgt aufgrund der Eindeutigkeit der Primfaktorzerlegung
(2) folgt aus $\forall n \in T_a \exists q \in P_a : q \mid n$
(3) folgt aus Definition 1.4.2
(4) folgt aus Definition von \mathbb{Z}_m^* als zu m teilerfremde Untermenge von \mathbb{Z}_m

Aufgabe 7

E	G	O	M	N	S	T	R
m	o	r	g	e	n	s	t

A	H	N	U	T	G	O	D
u	n	d	h	a	t	g	o

M	M	D	L	U	N	D	I
l	d	i	m	m	u	n	d

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 2 & 1 & 6 & 7 & 8 & 3 \end{pmatrix}$$

Aufgabe 8

$(\mathbb{Z}_{13}^*, \cdot)$ hat folgende 6 Untergruppen :

$$\begin{aligned}
 \langle 2 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} &= \langle 6 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} = \langle 7 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} = \langle 11 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} = (\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}, \cdot) \\
 \langle 1 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} &= (\{1\}, \cdot) \\
 \langle 3 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} &= \langle 9 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} = (\{1, 3, 9\}, \cdot) \\
 \langle 4 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} &= \langle 10 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} = (\{1, 3, 4, 9, 10, 12\}, \cdot) \\
 \langle 5 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} &= \langle 8 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} = (\{1, 5, 8, 12\}, \cdot) \\
 \langle 12 \rangle_{(\mathbb{Z}_{13}^*, \cdot)} &= (\{1, 12\}, \cdot)
 \end{aligned}$$

$\langle a \rangle_G$ sei die von a in G erzeugte Untergruppe, $\{a, \dots, n\}$ sei $\{[a]_{13}, \dots, [n]_{13}\}$

Die Lösungen wurden mittels folgendem Perl-Aufrufs ermittelt :

```
perl -e 'foreach $a (1..12) { my (@s, $i); while (++$i) {
  $s = $a**$i%13; (grep { $s == $_ } @s) ? last : push @s, $s }
  print $a, " : ", join (" ", sort {$a <=> $b} @s), "\n" }'
```

Aufgabe 9

(a) $extended_euclid(899, 493) = (29, -6, 11)$

(b) $x_0 = 6, x_1 = 16, x_2 = 26, x_3 = 36, x_4 = 46$

Zur Lösung beider Aufgaben wurde folgendes Programm verwendet :

```
#!/usr/local/bin/perl
use strict; no strict 'refs';

sub extended_euclid {
  $_[1] or return $_[0], 1, 0;
  my ($d, $x, $y) = extended_euclid ($_[1], $_[0] % $_[1]);
  $d, $y, $x - int($_[0] / $_[1]) * $y;
}

sub loese_mod_eg {
  my ($d, $x, $y) = extended_euclid ($_[0], $_[2]);
  $_[1] % $d ? undef : map { ($x * $_[1] / $d % $_[2] + $_ * $_[2]
    / $d) % $_[2] } 0..$d-1;
}

print join (', ', &{$ARGV[0]} (splice @ARGV, 1)), "\n";
```

(mit den Parametern `extended_euclid 899 493` bzw. `loese_mod_eg 35 10 50`)