$m = m_1 \cdot m_2 \cdot m_3 = 20 \cdot 9 \cdot 7 = 1260$

$M_1 = \frac{m}{m_1} = \frac{1260}{20} = 9 \cdot 7 = 63$, $M_2 = \frac{1260}{9} = 20 \cdot 7 = 140$

$M_3 = \frac{1260}{7} = 20 \cdot 9 = 180$

Erw. euklidischer Algorithmus liefert:

$1 = ggT(M_1, m_1) = 7 \cdot 63 - 22 \cdot \underset{m_1}{20} \Rightarrow \tilde{M}_1 = 7$

$1 = ggT(M_2, m_2) = 2 \cdot 140 - 31 \cdot 9 \Rightarrow \tilde{M}_2 = 2$

$1 = ggT(M_3, m_3) = 3 \cdot 180 - 77 \cdot 7 \Rightarrow \tilde{M}_3 = 3$

$\Rightarrow x = \sum_{j=1}^{3} M_j \cdot \tilde{M}_j \cdot a_j = 63 \cdot 7 \cdot 2 + 140 \cdot 2 \cdot 6 + 180 \cdot 3 \cdot 5$

$= \underline{5262} \equiv 222 \mod \underset{\underset{1260}{\shortparallel}}{m}$

Was passiert, wenn die m_i nicht paarweise teilerfremd sind?

Beispiel 4.32

(a) Betrachte die simultane Kongruenz $\begin{array}{l} x \equiv 2 \mod 10 = 2 \cdot 5 \\ x \equiv 3 \mod 14 = 2 \cdot 7 \end{array}$

Es ist $ggT(10, 14) = 2$

Die erste Kongruenz liefert, dass $x \equiv 0 \mod 2$ ist

Die zweite Kongruenz liefert, dass $x \equiv 1 \mod 2$ ist

Da $0 \neq 1 \mod 2$ hat die simultane Kongruenz keine Lsg.

(b) Betrachte $\left.\begin{array}{l} x \equiv 3 \mod 45 = 9 \cdot 5 \\ x \equiv 7 \mod 756 = 9 \cdot 84 \end{array}\right\} ggT(45, 756) = 3^2 = 9$

Wegen $7 \not\equiv 3 \mod 9$ folgt wie in (a), dass keine Lsg. existiert.

Es gibt also, falls die m_i in der simultanen Kongruenz nicht teilerfremd sind 2 Möglichkeiten:

1) Die einzelnen Kongruenzen widersprechen sich & es existiert daher keine Lösung. Dies stellt man fest,

indem man die indizierten Kongruenzen modulo
$ggT(m_1, \ldots, m_r)$ betrachtet.

2) Widersprechen sich die einzelnen Kongruenzen nicht, so kann man die simultane Kongruenz durch ein dazu "äquivalentes" System von Kongruenzen ersetzen. In diesem sind dann die "neuen m_i" paarweise teilerfremd.

Beispiel 4.33 20.06.18

Wir betrachten die simultane Kongruenz

(1) $x \equiv 7 \mod 200 = 5^2 \cdot 8$

(2) $x \equiv 82 \mod 375 = 5^3 \cdot 3$

Es ist $ggT(200, 375) = 5^2 = 25$ und da

$$7 \equiv \underbrace{82}_{\underbrace{75+7}_{=3\cdot 25}} \mod 5^2 = ggT(200, 375)$$

ist das System von Kongruenzen konsistent.

Nach dem CRS ist die erste Kongruenz (1) äquivalent zu:

(1a) $x \equiv 7 \mod 5^2$

(1b) $x \equiv 7 \mod 8$

Die zweite Kongruenz (2) ist nach dem CRS äquivalent zu

(2a) $x \equiv 82 \mod 5^3$

(2b) $x \equiv 82 \equiv 1 \mod 3$

Da "(1a) $\Rightarrow$ (2a)" ist insgesamt das System (1), (2) äquivalent zu:

$x \equiv 82 \mod 5^2$

$x \equiv 7 \mod 8$

$x \equiv 1 \mod 3$

Die neuen $\tilde{m}_i$'s sind alle teilerfremd & wir können daher das Verfahren aus Satz 4.29 anwenden.

Man findet so $x = 1207$.

Diese Lösung ist eindeutig modulo $kgV(m_i) = 5^3 \cdot 8 \cdot 3$

$$= \tilde{m}_1 \cdot \tilde{m}_2 \cdot \tilde{m}_3$$

$$= 3000$$

Mit dem CRS können wir nun den folgenden Satz zeigen:

Satz 4.34 (Multiplikativität der φ-Funktion)

(a) Seien $m_1, m_2 \in \mathbb{N}$ mit $ggT(m_1, m_2) = 1$. Dann ist
$\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$

(b) Sei p eine Primzahl & $r \in \mathbb{N}^*$, dann ist
$\varphi(p^r) = p^{r-1} \cdot (p-1) \quad \left(= p^r - \frac{p^r}{p}\right)$

(c) Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{p \in P} p^{n_p}$
Dann ist $\varphi(n) = \prod_{p \in P} \left(p^{n_p - 1} \cdot (p-1)\right) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

<u>Beweis:</u>

zu a) $a \in \mathbb{Z}$ ist genau dann teilerfremd zu $m = m_1 \cdot m_2$, wenn $ggT(a, m_1) = 1$ und $ggT(a, m_2) = 1$ ist.

Dies bedeutet, dass die Abbildung Φ (vgl. Bem. 4.30)
$\Phi : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/m_1\mathbb{Z})^* \times (\mathbb{Z}/m_2\mathbb{Z})^*$ wohldefiniert.

Nach dem CRS ist Φ bijektiv (vgl. Bem. 4.30)

Insb. ist $\varphi(m_1, m_2) = |(\mathbb{Z}/m\mathbb{Z})^*| \overset{\Phi \text{ bij}}{=} |(\mathbb{Z}/m_1\mathbb{Z})^*| \cdot |(\mathbb{Z}/m_2\mathbb{Z})^*|$

Dies zeigt (a).

zu b) Hier bemerken wir, dass $0 < a \leq p$ genau dann teilerfremd zu p^r ist, wenn a teilerfremd zu p ist, also genau dann wenn $p \nmid a$.

Es gibt genau p^{r-1} Zahlen $0 < a \leq p^r$ mit $p \mid a$, nämlich a's von der Form $a = j \cdot p$ mit $j = 1, \dots, p^{r-1}$

$\Rightarrow \varphi(p^r) = p^r - |\{0 < a \leq p^r \mid \underbrace{ggT(a,p) \neq 1}_{\Leftrightarrow p \mid a}\}|$

$= p^r - p^{r-1}$

zu c) folgt direkt aus a) & b). $\boxtimes$

Primitivwurzeln

Sei $m \in \mathbb{N}$ & $a \in \mathbb{Z}$ mit $ggT(a,m) = 1$ ($\Rightarrow a \in (\mathbb{Z}/m\mathbb{Z})^*$)

Wir haben bereits $ord_m(a) = \min\{r \mid a^r \equiv 1 \bmod m\}$

definiert & gesehen, dass $ord_m(a) \mid \varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$

Definition 4.35

Sei $m \in \mathbb{N}$ & $a \in \mathbb{Z}$ mit $ggT(a,m) = 1$. Die Zahl a heißt Primitivwurzel modulo m, falls $ord_m(a) = \varphi(m)$.

Beispiel 4.36

a) $m = 7$, also $\varphi(m) = 6$

a	1	2	3	4	5	6
$ord_7(a)$	1	3	6	3	6	2

$\rightsquigarrow a = 3$ & $a = 5$ sind Primitivwurzeln modulo 7

b) $m = 12$, also $\varphi(m) = \varphi(3) \cdot \varphi(4) = 2 \cdot 2 = 4$

a	1	5	7	11
$ord_{12}(a)$	1	2	2	2

$\leftarrow$ ist ein reduziertes Restsystem modulo 12 nach Bsp. 4.19

$\Rightarrow$ Es existiert keine Primitivwurzel mod 12

Eine Primitivwurzel modulo m existiert also genau dann, wenn $(\mathbb{Z}/m\mathbb{Z})^*$ zyklisch ist, also von <u>einem</u> Element erzeugt ist.

Lemma 4.37

Ist a eine Primitivwurzel modulo m, so ist

$R = \{a, a^2, \ldots, a^{\varphi(m)}\}$ ein reduziertes Restsystem modulo m

<u>Beweis:</u>

Sei $1 \leq i < j \leq \overset{ord(a)}{\varphi(m)}$. Per Def. der Ordnung ist $a^{j-i} \not\equiv 1 \bmod m$

$\Rightarrow a^j \not\equiv a^i \bmod m$

Es ist $ggT(a^i, m) = 1 \;\forall i$ & da $|R| = \varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$

folgt, dass R ein reduziertes Restsystem modulo m ist $\square$

Eine Primitivwurzel erzeugt also die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^*$

Lemma 4.38

Seien $m \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $ggT(a,m) = 1$.

Für alle $k \in \mathbb{N}$ gilt: $ord_m(a^k) = \frac{ord_m(a)}{ggT(ord_m(a), k)}$

Beweis: Übung!

Beispiel 4.39

Nach Bsp. 4.36 ist $a = 3$ eine Primitivwurzel modulo 7

k	1	2	3	4	5	6
a^k	$3^1 = 3$	$3^2 \equiv 2$	6	4	5	1
$ord_7(a^k)$	6	3	2	3	6	1

Wir möchten zeigen, dass falls $m = p$ eine Primzahl ist, stets eine Primitivwurzel modulo p existiert. Der nächste Satz wird dabei helfen.

Bemerkung 4.40

Im Beweis des nächsten Satzes werden wir folgende (bis jetzt) unbewiesene Tatsache verwenden:

Sei K ein Körper und $f = \sum_{i=0}^{d} a_i x^i \in K[x]$ ein Polynom mit Koeffizienten $a_i \in K$. Dann hat f höchstens $Grad(f) = d$ viele Nullstellen in K. Für $K = \mathbb{R}, \mathbb{C}$ kennt man diesen Satz aus der Analysis. Für beliebige Körper z.B. $K = \mathbb{Q}$ oder $K = \mathbb{Z}/p\mathbb{Z}$ (p = Primzahl) kann man dies ebenfalls mit Hilfe der Polynomdivision beweisen. (dazu evtl. mehr in den Übungen)

Satz 4.41

Sei p eine Primzahl & d ein Teiler von $(p-1)$. Dann hat die Kongruenz $x^d \equiv 1 \mod p$ genau d Lösungen modulo p.

Beweis:

$d \mid (p-1) \Rightarrow d \cdot e = (p-1)$. Analog zu Blatt 6 A4 findet man

$$x^{p-1} - 1 = (x^d - 1)(x^{d \cdot (e-1)} + x^{d \cdot (e-2)} + \dots + x^d + 1)$$
$$=: (x^d - 1) \cdot g(x) \quad , g(x) \text{ Polynom in } x$$

Nach dem kleinen Satz von Fermat (4.22) hat die Kongruenz $x^{p-1} - 1 \equiv 0 \mod p$ genau $(p-1)$ Lösungen, nämlich genau die Elemente von $(\mathbb{Z}/p\mathbb{Z})^*$.

[Anders ausgedrückt: $x^p - 1$ aufgefasst als Polynom in $K[x]$ für $\mathbb{Z}/p\mathbb{Z}$ hat genau $(p-1)$ Nullstellen, nämlich die Elemente von $(\mathbb{Z}/p\mathbb{Z})^*$]

Fassen wir $g(x)$ als Polynom in $K[x]$ auf (für $K = \mathbb{Z}/p\mathbb{Z}$) so sagt Bem. 4.40, dass $g(x)$ höchstens $\text{Grad}(g) = p-1-d$ viele Nullstellen hat.

Die Kongruenz $g(x) \equiv 0 \mod p$ hat also höchstens $(p-1)$ Lösungen modulo p

$\Rightarrow$ Es gibt mindestens d Elemente $a \in (\mathbb{Z}/p\mathbb{Z})^*$ mit $g(a) \not\equiv 0 \mod p$ und $a^{p-1} \equiv 1 \mod p$.

Da $x^d - 1 \equiv 0 \mod p$ nach Bem. 4.40 höchstens d Lösungen besitzt (und $x^{p-1} - 1 = (x^d - 1) \cdot g(x)$) schließen wir, dass $x^d - 1 \equiv 0 \mod p$ genau d Lösungen hat modulo p.

Satz 4.42

Sei p eine Primzahl & d ein Teiler von $(p-1)$.

Für $\psi(d) := |\{1 \leq a < p \mid \text{ord}_p(a) = d\}|$ gilt $\psi(d) = \varphi(d)$.

Korollar 4.43

Sei P eine Primzahl, dann existiert eine Primitivwurzel modulo p.

Beweis:

$\psi(p-1)$ ist per Definition von ψ und der Definition von Primitivwurzel genau die Anzahl der Primitivwurzeln modulo p.

Nach Satz 4.42 ist $\psi(p-1) = \varphi(p-1)$ & wegen der Multiplikativität von φ (4.34) ist $\varphi(p-1) > 0$.

Es existiert also eine Primitivwurzel modulo p. $\boxtimes$

Beweis von 4.42:

Wir zeigen zunächst, dass $\psi(d) = \varphi(d)$ gilt, falls $\psi(d) > 0$.

Wegen $\psi(d) > 0$ existiert $a \in \{1, \dots, p-1\}$ mit $\mathrm{ord}_p(a) = d$.

Analog zum Beweis von 4.37 sehen wir, dass

$a^i \not\equiv a^j \bmod p$ für $1 < i < j \leq \varphi(p) = p-1$.

Da nach Voraussetzung die $\mathrm{ord}_p(a) = d$ gilt:

$(a^i)^d \equiv (a^d)^i \equiv 1^i \equiv 1 \bmod p$

$\Rightarrow$ Für $i = 1, \dots, d$ ist a^i eine Lösung von $x^d \equiv 1 \bmod p$.

Nach Satz 4.41 hat die Kongruenz $x^d \equiv 1 \bmod p$ genau d Lösungen modulo p. Diese Lösungen sind also $a, a^2, \dots, a^d$. ($\rightsquigarrow \psi(d) = d$)

Wegen Lemma 4.38 sehen wir, dass $\mathrm{ord}_p(a^i) = d$ genau dann, wenn $i \in (\mathbb{Z}/d\mathbb{Z})^*$ ($\Leftrightarrow \mathrm{ggT}(i,d) = 1$)

Also ist die Anzahl solcher i's genau $|(\mathbb{Z}/d\mathbb{Z})^*| = \varphi(d)$.

Wir sehen, dass $\psi(d) = \varphi(d)$, falls $\psi(d) > 0$.

Als nächstes schließen $\psi(d) = 0$ aus.

Nach Lemma 4.25 ist $\mathrm{ord}_p(a)$ ein Teiler von $\varphi(p) = p-1$.

$\Rightarrow \sum_{d \mid (p-1)} \psi(d) = |(\mathbb{Z}/p\mathbb{Z})^*| = p-1$ (jedes Element in $(\mathbb{Z}/p\mathbb{Z})^*$ hat eine Ordnung $d \geq 1$ & diese teilt $p-1$)

Auf der anderen Seite gilt nach Lemma 4.27, dass

$$\sum_{d|(p-1)} \varphi(d) = p-1$$

Wir bemerken zudem, dass $\psi(d) \leq \varphi(d)$ $\forall d$ Teiler von $(p-1)$:

Falls $\psi(d) = 0$ ist dies offensichtlich richtig.

Falls $\psi(d) > 0$ so haben wir bereits gezeigt, dass $\psi(d) = \varphi(d)$.

Wir schließen, dass

$$(p-1) = \sum_{d|(p-1)} \psi(d) \leq \sum_{d|(p-1)} \varphi(d) = (p-1)$$

Und da $\psi(d) \leq \varphi(d)$ $\forall d$ ist, kann dies nur gelten, wenn

$\psi(d) = \varphi(d)$ $\forall d$ mit $d \mid (p-1)$. $\square$

Der obige Satz sagt uns lediglich, dass die Anzahl der Primitivwurzeln modulo p genau $p-1$ ist, aber nicht, wie man Primitivwurzeln findet. Hat man jedoch eine Primitivwurzel a modulo p so sagt der obige Beweis, dass alle weiteren Primitivwurzeln von der Form a^i mit $ggT(i, p-1) = 1$ sind.

\# solcher i's ist $\varphi(p-1)$.

Beispiel 4.44

Wir haben gesehen, dass 3 und 5 Primitivwurzeln mod 7 sind. In der Tat ist $\varphi(7-1) = \varphi(6) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = 2$

$\{ i \mid ggT(i, \underbrace{7-1}_{=6}) = 1 \} = \{1, 5\}$

$3^5 \equiv 5 \mod 7$ und $5^5 \equiv 3 \mod 7$.