Aufgabe: Hier beziehen wir uns auf ein ganz einfaches Konzept von Einwegfunktion:

f bijektiv, $f \in P$, $f^{-1} \notin P$. In diesem Sinne seien f und g Einwegfunktionen.
Betrachte die Hintereinanderanwendung von f, gefolgt von g; dies sei die Funktion h.
(Meine Notation hierfür: $h = f \circ g$ – nicht in Übereinstimmung mit manchen Mathe-Lehrbüchern).

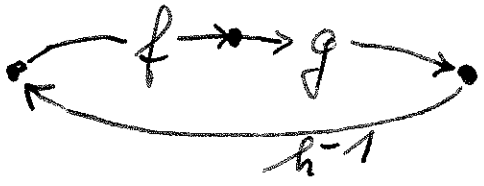
Man zeige, dass auch h eine Einwegfunktion ist!

Antwort: Erstens, $h = f \circ g$ kann effizient berechnet werden durch Hintereinanderausführung des Algorithmus für f, gefolgt von dem für g. Notation: $M_h = M_f ; M_g$

Zweitens, h ist bijektiv, da es f und g sind.

Drittens, $h^{-1} \notin P$. Angenommen, das wäre nicht der Fall, also $h^{-1} \in P$. Dann kann man auch f invertieren mittels $f^{-1} = g \circ h^{-1}$ bzw g invertieren mittels $g^{-1} = h^{-1} \circ f$. Widerspruch.

Skizze:



Aufgabe: Du hast vor, ein Paper zu veröffentlichen, das den Wert der Rechenoperation $x \circ y$ bekannt gibt. (Berechnungen mit „$\circ$" sind zur Zeit besonders hipp in der Wissenschaftsszene). Andererseits ist die Berechnung von $z := x \circ y$ auch ganz besonders schwierig. Dein Papers-intelligenter Zimmernachbar im Institut kann besonders gut $\bullet$-Berechnungen durchführen. Wie kommst du mit Hilfe einer homophonen Einwegfunktion mit Falltür zu deiner gewünschten Veröffentlichung von „$z = x \circ y$"?

Antwort: Die betreffende Einwegfunktion sei f. Du berechnest $x' = f(x)$ und $y' = f(y)$ und bittest deinen Zimmernachbarn, „mal eben" $x' \bullet y'$ auszurechnen. Wegen der Homomorphie-Eigenschaft von f ist $x' \bullet y' = f(x) \bullet f(y) = f(x \circ y)$. Für dich ist die Funktion f invertierbar. Du kannst dann also aus $f(x \circ y)$ den gesuchten Wert $x \circ y$ berechnen.

Aufgabe: Für jedes n ist $(\mathbb{Z}_n^*, *)$ eine Gruppe. Man gebe die „Multiplikationstafel" für $\mathbb{Z}_{14}^*$ an und bestimme aus dieser die multiplikativen Inversen und die Quadratzahlen.

Lösung: Es ist $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$, d.h. $\varphi(14) = 6$

Multiplikationstafel:

$*$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

Inverse:

$1 \leftrightarrow 1$

$3 \leftrightarrow 5$

$9 \leftrightarrow 11$

$13 \leftrightarrow 13$

Quadrate bilden:

$$1^2 = 1\,,\ 3^2 = 9\,,\ 5^2 = 11\,,\ 9^2 = 11\,,$$
$$11^2 = 9\,,\ 13^2 = 1$$

Quadratzahlen sind also:

1 mit den Quadratwurzeln 1 und 13

9 〃 〃 〃 3 und 11

11 〃 〃 〃 5 und 9

Aufgabe: Gib $\mathbb{Z}_{15}^*$ an und bestimme $\varphi(15)$:

Antwort: $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$\varphi(15) = |\mathbb{Z}_{15}^*| = 8.$

Aufgabe: Nehmen wir an, $\mathbb{Z}_n^*$ ist eine zyklische Gruppe, d.h. es gibt mindestens eine Zahl a mit $\{a^1, a^2, a^3, \ldots, a^{\varphi(n)}\} = \mathbb{Z}_n^*$.
Wieviele solche erzeugende Elemente besitzt die Gruppe $\mathbb{Z}_n^*$ dann insgesamt?

Antwort: Jede beliebige Zahl $b \in \mathbb{Z}_n^*$ kann als eine Potenz von a dargestellt werden: $b = a^i$.
Betrachten wir nun $b^1, b^2, b^3, \ldots = a^i, a^{2i}, a^{3i}, \ldots$
Es stellt sich die Frage, ob diese Folge sämtliche $\varphi(n)$-vielen Elemente von $\mathbb{Z}_n^*$ tatsächlich durchläuft, bevor sie sich wiederholt. Das ist genau dann der Fall, wenn i und $\varphi(n)$ teilerfremd sind, also $i \in \mathbb{Z}_{\varphi(n)}^*$.
Dies trifft für $\varphi(\varphi(n))$ viele i's zu.

Das heißt, die erzeugenden Elemente von $\mathbb{Z}_n^*$ sind genau die Zahlen $\{a^i \mid i \in \mathbb{Z}_{\varphi(n)}^*\}$.

Für n Primzahl gilt, dass $\mathbb{Z}_n^*$ tatsächlich zyklisch ist, daher hat $\mathbb{Z}_n^*$ genau $\varphi(n-1)$ viele Erzeuger (denn $\varphi(n) = n-1$).

Beispiel: $\mathbb{Z}_{11}^*$ ist zyklisch. Ein Erzeuger ist $a=2$:

$a^1, a^2, a^3, \ldots, a^{10} = 2, 4, 8, 5, 10, 9, 7, 3, 6, 1$

Teilerfremd zu $n-1 = 10$ sind die Zahlen $1, 3, 7, 9$.

Daher sind sämtliche Erzeuger von $\mathbb{Z}_{11}^*$ die Zahlen $a^1 = 2$, $a^3 = 8$, $a^7 = 7$, $a^9 = 6$.

Probe:

$8^1, 8^2, 8^3, \ldots, 8^{10} = 8, 9, 6, 4, 10, 3, 2, 5, 7, 1$

$7^1, 7^2, 7^3, \ldots, 7^{10} = 7, 5, 2, 3, 10, 4, 6, 9, 8, 1$

$6^1, 6^2, 6^3, \ldots, 6^{10} = 6, 3, 7, 9, 10, 5, 8, 4, 2, 1$

Nochmals zusammengefasst: Eine Gruppe der Form $(\mathbb{Z}_n^*, *)$ ist entweder nicht zyklisch und hat 0 Erzeuger, oder sie ist zyklisch, dann hat sie $\varphi(\varphi(n))$ viele Erzeuger.

Aufgabe: Man zeige, dass in jeder Gruppe $(\mathbb{Z}_n^*, *)$ immer $(n-1)^2 = 1$ gilt.

Beweis:

$$(n-1)^2 = \underbrace{n^2}_{\equiv 0} - \underbrace{2n}_{\equiv 0} + 1 \equiv 1 \pmod{n}$$

Anders ausgedrückt: es gilt immer $(-1)^2 = 1$.

Aufgabe: Man teste bei $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$ für jedes Element einzeln, ob es ein Erzeuger (Primitivwurzel) ist.

Antwort:

$1^1, 1^2, 1^3, 1^4, \ldots$	$=$	$1, 1, 1, \ldots$	kein Erzeuger (Periode = 1)
$3^1, 3^2, 3^3, 3^4, 3^5, 3^6$	$=$	$3, 9, 13, 11, 5, 1$	Erzeuger
$5^1, 5^2, 5^3, 5^4, 5^5, 5^6$	$=$	$5, 11, 13, 9, 3, 1$	Erzeuger
$9^1, 9^2, 9^3, 9^4, 9^5, 9^6$	$=$	$9, 11, 1, 9, 11, 1$	kein Erzeuger (Periode = 3)
$11^1, 11^2, 11^3, 11^4, 11^5, 11^6$	$=$	$11, 9, 1, 11, 9, 1$	kein Erzeuger (Periode = 3)
$13^1, 13^2, 13^3, 13^4, 13^5, 13^6$	$=$	$13, 1, 13, 1, 13, 1$	kein Erzeuger (Periode = 2)

Aufgabe: Sei $n = p \cdot q$ wobei p und q zwei verschiedene Primzahlen sind.

Zeige, dass $\underbrace{\varphi(n)}_{\text{Anzahl der teilerfremden Zahlen } x \in \{1,\dots,n\}} = (p-1)\cdot(q-1)$

Lösung:

Zunächst stehen alle Zahlen $1, 2, 3, \dots, n = p \cdot q$ als Kandidaten, teilerfremd zu n zu sein, zur Verfügung. Wir streichen nun alle Vielfachen von p heraus, also die Zahlen: $\underbrace{p, 2p, 3p, \dots, qp = n}_{q\text{-viele}}$

Ferner streichen wir die Vielfachen von q:

$\underbrace{q, 2q, 3q, \dots, p \cdot q = n}_{p\text{-viele}}$ Die einzige Übereinstimmung liegt in der Zahl pq vor. Daher ist die Anzahl der verbleibenden Zahlen:

$$n - q - p + 1 = p \cdot q - q - p + 1$$

$$= (p-1)\cdot(q-1)$$

Aufgabe: 7 ist Primzahl, $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$.
Die Zahl 3 ist ein Erzeuger von $\mathbb{Z}_7^*$ (also $\langle 3 \rangle = \mathbb{Z}_7^*$).
Man bestimme die diskreten Logarithmen von
$y = 1, 2, 3, 4, 5, 6$ zur Basis 3.

Antwort: Es ist $3^0, 3^1, 3^2, 3^3, 3^4, 3^5 = 1, 3, 2, 6, 4, 5$
Also ist der Logarithmus von
$y = 1, 2, 3, 4, 5, 6$ gleich $0, 2, 1, 4, 5, 3$

Beispiel: Die Funktion $f(x) = 627^x \bmod 941$

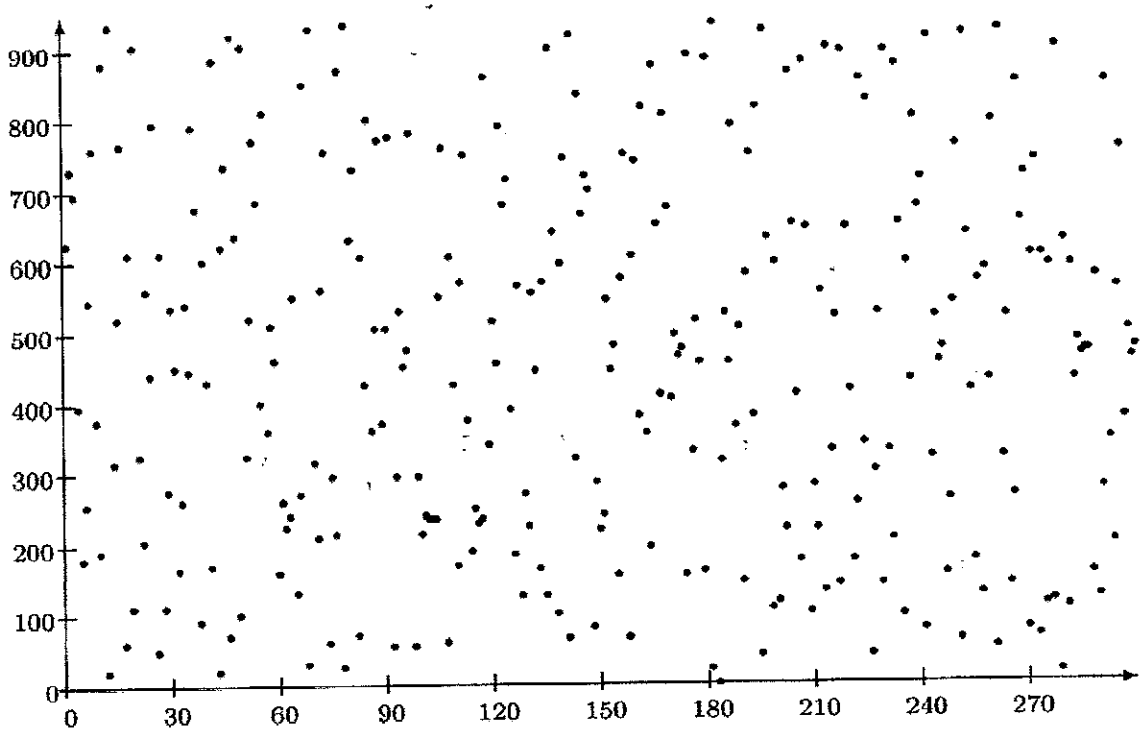


Figure 2.2: Powers $627^i \bmod 941$ for $i = 1, 2, 3, \ldots$

Aufgabe: Du musst den Diskreten Logarithmus berechnen: gegeben n (Primzahl) und $a \in \mathbb{Z}_n^*$ (Erzeuger) sowie $y \in \mathbb{Z}_n^*$. Gesucht ist x so dass $y \equiv a^x \pmod n$. Die Zahlen bestehen aus Hunderten von Dezimalziffern.

Ein Orakel behauptet, für $\frac{1}{100}$ aller $z \in \mathbb{Z}_n^*$ den diskreten Logarithmus von z berechnen zu können. (Leider ist das fragliche y nicht unter diesen z's.)

Gib einen effizienten Algorithmus an, der mit Hilfe dieses Orakels den diskreten log. von y berechnen kann! (Hinweis: probabilistischer Algorithmus)

Antwort: Wähle j zufällig und frage das Orakel, ob es den Diskr. log von $z = y \cdot a^j \bmod n$ berechnen kann. Wenn ja (was nach ca 100 Versuchen passieren wird), so liefert das Orakel eine Zahl i so dass $a^i \equiv y \cdot a^j \pmod n$

$\iff a^i \cdot a^{-j} \equiv y \pmod n \iff a^{i-j} \equiv y \pmod n$

Die Lösung ist also $x = i - j$ ← Beachte: diese Rechnung modulo $n-1$.

Aufgabe: Man gebe die Anzahl der erzeugenden Elemente an bei $\mathbb{Z}_5^*, \mathbb{Z}_6^*, \dots, \mathbb{Z}_{21}^*$.

Antwort:

5: $\varphi(\varphi(5)) = \varphi(4) = 2$

6: $\varphi(\varphi(6)) = \varphi(2) = 1$

7: $\varphi(\varphi(7)) = \varphi(6) = 2$

8: 0, da $\mathbb{Z}_8^*$ nicht zyklisch

9: $\varphi(\varphi(9)) = \varphi(6) = 2$

10: $\varphi(\varphi(10)) = \varphi(4) = 2$

11: $\varphi(\varphi(11)) = \varphi(10) = 4$

12: 0, da $\mathbb{Z}_{12}^*$ nicht zyklisch

13: $\varphi(\varphi(13)) = \varphi(12) = 6$

14: $\varphi(\varphi(14)) = \varphi(6) = 2$

15: 0, da $\mathbb{Z}_{15}^*$ nicht zyklisch

16: 0, da $\mathbb{Z}_{16}^*$ nicht zyklisch

17: $\varphi(\varphi(17)) = \varphi(16) = 8$

18: $\varphi(\varphi(18)) = \varphi(6) = 2$

19: $\varphi(\varphi(19)) = \varphi(18) = 6$

20: 0, da $\mathbb{Z}_{20}^*$ nicht zyklisch

21: 0, da $\mathbb{Z}_{21}^*$ nicht zyklisch.

Vergleiche hierzu:

Satz (Gauß): Die Gruppe $(\mathbb{Z}_n^*, *)$ ist genau dann zyklisch, wenn n eine der Formen hat: $1, 2, 4, p^k, 2p^k$ wobei p eine ungerade Primzahl ist, $k \in \mathbb{N}$.

Ohne Beweis.

Zusammenstellung von Notationen und Fakten

- Die Ordnung einer Gruppe G ist die Anzahl ihrer Elemente: $|G|$

- Die Ordnung eines Elements $a \in G$ ist die kleinste Zahl i so dass $a^i = 1$ (wobei 1 das neutrale Element der Gruppe ist, und $a^i = \underbrace{a \circ a \circ \dots \circ a}_{i\text{-mal}}$).

- Eine endliche Gruppe G ist zyklisch, falls es ein Element $a \in G$ gibt, dessen Ordnung gleich $|G|$ ist. Das bedeutet:

$$G = \{\underbrace{a^1, a^2, a^3, \dots}_{\text{alle voneinander verschieden}}, \underbrace{a^{|G|}}_{=1}\}$$

- U ist eine Untergruppe von G, falls $U \subseteq G$ und falls U für sich betrachtet eine Gruppe ist. D.h: neutrales Element $\in U$, Abgeschlossenheit, inverse Elemente $\in U$.

- Satz von Lagrange:

U Untergruppe von G $\Rightarrow$ $|U|$ teilt $|G|$.

Anwendung in der Algorithmik/Kryptographie:
Ein probabilistischer Algorithmus wählt ein Element $a \in G$ (oft ist $G = \mathbb{Z}_n^*$) zufällig aus und führt anschließend eine Berechnung durch. Manche a führen evtl. auf ein falsches Ergebnis. Wenn man ~~die~~ zeigen kann, dass sich solche „bösartigen" a alle in einer echten Untergruppe U von G befinden, so folgt mit dem Satz von Lagrange, dass $|U| \leq \frac{|G|}{2}$. Also gilt:

$$P(\text{Algorithmus liefert falsches Ergebnis}) \leq \frac{1}{2}.$$

- Für jedes $a \in G$ ist $\langle a \rangle := \{a^0 (= 1), a^1, a^2, \dots\}$ eine Untergruppe von G. G ist zyklisch, falls $\exists a \in G: \langle a \rangle = G$.

Bsp: $G = \mathbb{Z}_{14}^*$, $\langle 9 \rangle = \{1, 9, 11\}$

	1	9	11
1	1	9	11
9	9	11	1
11	11	1	9

Zur Berechnung von $\varphi(n)$:

– Bisher wissen wir:

n Primzahl $\Rightarrow \varphi(n) = n-1$

$n = p \cdot q$ (p, q verschiedene Primzahlen)

$\Rightarrow \varphi(n) = (p-1)\cdot(q-1)$

Es fehlen noch einige Fälle, um für beliebiges n $\varphi(n)$ ausrechnen zu können.

Es gelten folgende Fakten (Beweise später):

Falls $n = x \cdot y$ und x, y sind teilerfremd ($ggT(x,y)=1$),

dann gilt: $\varphi(n) = \varphi(x) \cdot \varphi(y)$.

Falls $n = p^k$ (p Primzahl), dann ist $\varphi(n) = p^k - p^{k-1}$

$= p^{k-1}(p-1)$

Insgesamt ergibt sich somit:

Falls n die (eindeutige) Primfaktorisierung

$n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$ hat, so ist

$$\varphi(n) = \varphi(p_1^{i_1}) \cdot \varphi(p_2^{i_2}) \cdots \varphi(p_k^{i_k}) = (p_1-1)p_1^{i_1-1}(p_2-1)p_2^{i_2-1}\cdots(p_k-1)p_k^{i_k-1}$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

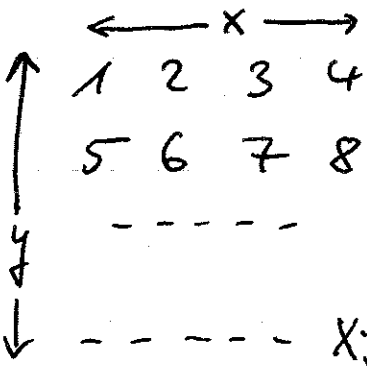
Beweis von $\varphi(p^k) = p^k - p^{k-1}$ (p Primzahl)

Zunächst stehen die Zahlen $1, 2, \ldots, p^k$ grundsätzlich zur Verfügung, teilerfremd zu p^k zu sein. Gestrichen werden müssen alle Vielfachen von p: $p, 2p, \ldots, p^{k-1} \cdot p$

Dies sind p^{k-1} Zahlen, also ist $\varphi(p^k) = p^k - p^{k-1}$. □

Beweis von $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ sofern $ggT(x,y) = 1$.

Wir tragen die Zahlen von 1, 2, bis $x \cdot y$ zeilenweise in eine $x \cdot y$ rechteckige Matrix ein:



Die Spalten enthalten jeweils Zahlen, die zueinander kongruent modulo x sind.

Als teilerfremd zu xy kommen nun alle Spalten gestrichen werden, die nicht in $\mathbb{Z}_x^*$ liegen; es verbleiben also $\varphi(x)$ Spalten.

Innerhalb einer Spalte durchlaufen die Zahlen ein vollständiges Restsystem modulo y, da mit Schrittweite x fortgezählt wird, und da $ggT(x,y) = 1$. Als teilerfremd zu xy kommen in jeder Spalte nur die Zahlen eines reduzierten Restsystems in Frage. Insgesamt sind es also $\varphi(x) \cdot \varphi(y)$ viele. □

Wir beschränken uns auf den Fall $n = p \cdot q$

Dann gilt:

$$n \text{ faktorisieren} \equiv_{\text{eff}} \varphi(n) \text{ berechnen}$$

Beweis: ($\varphi(n)$ berechnen $\leq_{\text{eff}}$ n faktorisieren)

Wenn man p und q kennt, kann man $\varphi(n) = (p-1)(q-1)$ berechnen.

(n faktorisieren $\leq_{\text{eff}}$ $\varphi(n)$ berechnen)

Wenn man $m := \varphi(n)$ kennt, so gilt:

$$m = (p-1)(q-1) = pq - p - q + 1 = n - p - \frac{n}{p} + 1$$

$$\Leftrightarrow \quad mp = np - p^2 - n + p$$

$$\Leftrightarrow \quad p^2 + (m-n-1) \cdot p + n = 0$$

$$p_{1,2} = \frac{n - m + 1 \pm \sqrt{(n-m+1)^2 - 4n}}{2}$$

Die beiden Lösungen sind p und q.