

Vorlesung

Effiziente Algorithmen und Komplexitätstheorie

Sommersemester 2008

Ingo Wegener

Wiederholung

Wir haben

- RSA-Kryptosystem gesehen
- verstanden, dass Sicherheit der Schwierigkeit der Faktorisierung beruht
- Implementierung von Chiffrierung und Dechiffrierung betrachtet
- effiziente Implementierung von schneller Potenzierung, ggT-Berechnung und multiplikativen Inversen besprochen
- gesehen, dass „Rate Zahl n und teste, ob n prim ist“ effizienter Algorithmus zur Bestimmung zufälliger Primzahlen ist, wenn Primzahltests effizient durchführbar sind
- erfahren, dass $\text{PRIMES} \in \text{P}$ gilt
- Plan, effizienten Algorithmus für PRIMES kennenzulernen, der **randomisiert** ist und **mit kleiner W'keit** zusammengesetzte Zahlen **fälschlich** als „vielleicht prim“ identifiziert

dafür hilfreich etwas Gruppen- und Zahlentheorie

Wiederholung Gruppentheorie

Definition 12.13

Menge G mit binärer Operation \circ heißt **Gruppe**, wenn gilt:

- $\forall a, b, c \in G: (a \circ b) \circ c = a \circ (b \circ c)$ (**Assoziativität**)
- $\exists e \in G: \forall a \in G: a \circ e = e \circ a = a$ (**neutrales Element**)
- $\forall a \in G: \exists b \in G: a \circ b = b \circ a = e$ (**inverse Elemente**)

Gilt zusätzlich $\forall a, b \in G: a \circ b = b \circ a$ (Kommutativität), so heißt (G, \circ, e) **abelsche Gruppe**.

Definition 12.14

Sei (G, \circ, e) Gruppe. $H \subseteq G$ heißt **Untergruppe**, wenn (H, \circ, e) Gruppe ist.

Zu einer Untergruppe H von G definieren wir Relation \sim_H durch
 $\forall a, b \in G: a \sim_H b :\Leftrightarrow b^{-1} \circ a \in H$

Wiederholung Gruppentheorie

Theorem 12.15

G endliche Gruppe, H Untergruppe von G .
 $|H| \mid |G|$

Definition 12.16

Sei (G, \circ, e) Gruppe, $a \in G$. Es ist $\langle a \rangle := \{a^i \mid i \in \mathbb{Z}\}$,
 $\text{ord}_G(a) := |\langle a \rangle|$ heißt **Ordnung** von a in G . a heißt **erzeugendes Element**, wenn $\langle a \rangle = G$ gilt. G heißt **zyklisch**, wenn G erzeugendes Element hat.

Theorem 12.18

Sei (G, \circ, e) Gruppe, $a \in G$ mit $\text{ord}_G(a) = n$ für ein $n \in \mathbb{N}$.

- 1 $\forall i \leq j: a^i = a^j \Leftrightarrow n \mid (j - i)$
- 2 $\langle a \rangle$ ist isomorph zu $(\mathbb{Z}_n, + \text{ mod } n, 0)$.

(Nur ganz wenig) Zahlentheorie

Erinnerung $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$

Definiere $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1\}$

Beobachtung für Primzahl n $\mathbb{Z}_N^* = \mathbb{Z}_n \setminus \{0\}$

Behauptung $(\mathbb{Z}_n^*, \cdot \text{ mod } n, 1)$ ist Gruppe
 denn 1 ist neutrales Element,
 unter $\cdot \text{ mod } n$ abgeschlossen,
 a^{-1} existiert für alle $a \in \mathbb{Z}_n^*$ ✓

Ordnung von a in $(\mathbb{Z}_n^*, \cdot \text{ mod } n, 1)$
 $\min \{i \geq 1 \mid a^i \equiv 1 \text{ mod } n\}$
 schreiben wir kurz als $\text{ord}_n(a)$

klar $a \in \mathbb{Z}_n^*$ erzeugendes Element $\Leftrightarrow \langle a \rangle = \{a^i \mid i \geq 0\} = \mathbb{Z}_n^*$

Beobachtung n prim $\Rightarrow \mathbb{Z}_n^*$ hat erzeugendes Element

Einige Begriffe

- $a \in \mathbb{Z}_n^*$ heißt **quadratischer Rest** modulo n ($a \in \text{QR}(n)$), wenn $x^2 \equiv a \pmod n$ Lösung in \mathbb{Z}_n^* hat
- Betrachte \mathbb{Z}_n^* für beliebiges n mit erzeugendem Element $g \in \mathbb{Z}_n^*$. $\text{index}_g(a) = \min \{i \geq 0 \mid g^i \equiv a \pmod n\}$ heißt **Index** von a
- $n \in \mathbb{N}$ heißt **quadratfrei**, wenn $\nu_p(n) \in \{0, 1\}$ für alle Primzahlen p gilt
- **Carmichael-Funktion** $\lambda: \mathbb{N} \rightarrow \mathbb{N}$ ist definiert durch $\lambda(n) = \min \{i \geq 1 \mid \forall a \in \mathbb{Z}_n^*: a^i \equiv 1 \pmod n\}$

so weit alles ziemlich abstrakt und inhaltsleer

Was machen wir nun?

erstmal etwas mit **Leben** füllen

Eigenschaften der Carmichael-Funktion

Fakt 12.19

Für alle ungeraden Primzahlen p und alle $e \in \mathbb{N}$ gilt

$$\lambda(e^p) = p^{e-1} \cdot (p-1).$$

Es ist $\lambda(2) = 1$, $\lambda(4) = 2$ und für alle $e \geq 3$ gilt

$$\lambda(2^e) = e^{e-2}.$$

Für alle n mit Primfaktorzerlegung $n = \prod_{p \text{ prim}} p^{\nu_p(n)}$ gilt

$$\lambda\left(\prod_{p \text{ prim}} p^{\nu_p(n)}\right) = \text{kgV}\left(p^{\nu_p(n)} \mid p \text{ prim}\right).$$

Über quadratische Reste

Theorem 12.20

$$\forall p \geq 3 \text{ prim: } |\text{QR}(p)| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}$$

Beweis

Erinnerung $a^2 \in \mathbb{Z}_p^*$ quadratischer Rest
 $x^2 \equiv a^2 \pmod{p}$ hat Lösung

klar lösbar $\Leftrightarrow (a+x) \cdot (a-x) \equiv 0 \pmod{n}$ lösbar

klar x mit $x \equiv -a \pmod{n}$ und $x \equiv a \pmod{n}$ **passt**

Fakt weil p Primzahl, gilt das auch nur für solche x
(\mathbb{Z}_p^* ist **nullteilerfrei**)

also $\text{QR}(p) = \left\{ x^2 \mid x = 1, 2, \dots, \frac{p-1}{2} \right\}$

also $|\text{QR}(p)| = (p-1)/2$



Über die Ordnung

Theorem 12.21

$$\forall a \in \mathbb{Z}_n^* : a^e \equiv 1 \pmod{n} \Leftrightarrow \text{ord}_n(a) \mid e$$

Beweis.

Definiere $j = e \bmod \text{ord}_n(a)$, $k = \lfloor e / \text{ord}_n(a) \rfloor$

also $e = k \cdot \text{ord}_n(a) + j$ mit $0 \leq j < \text{ord}_n(a)$

also $a^e = a^{k \cdot \text{ord}_n(a) + j} = a^{k \cdot \text{ord}_n(a)} \cdot a^j \equiv a^j \pmod{n}$

also $a^e \equiv 1 \pmod{n} \Leftrightarrow a^j \equiv 1 \pmod{n}$ mit $0 \leq j < \text{ord}_n(a)$

also $a^e \equiv 1 \pmod{n} \Leftrightarrow j = 0$

also $\text{ord}_n(a) \mid e$



Kleiner Satz von Fermat

Theorem 12.22

Sei p prim.

$$\forall a \in \mathbb{Z}_p^* : a^{p-1} \equiv 1 \pmod{p}$$

Beweis.

Erinnerung $\langle a \rangle = \{a^i \mid i \geq 0\}$
 $\text{ord}_p(a) = \min \{i \geq 1 \mid a^i \equiv 1 \pmod{p}\}$

also $|\langle a \rangle| = \text{ord}_p(a), a^{\text{ord}_p(a)} \equiv 1 \pmod{p}$

Beobachtung $(\langle a \rangle, \cdot \pmod{p}, 1)$ ist
 Untergruppe von $(\mathbb{Z}_p^*, \cdot \pmod{p}, 1)$

also $|\langle a \rangle| \mid |\mathbb{Z}_p^*|, \text{ord}_p(a) \mid p-1$
 wegen Theorem 12.15

also $p-1 = k \cdot \text{ord}_p(a)$ für ein $k \in \mathbb{N}$

also $a^{p-1} = a^{k \cdot \text{ord}_p(a)} \equiv 1 \pmod{p}$



Einen Moment!

Ist das hier „Elementare Zahlentheorie“ oder „Effiziente Algorithmen?“

Was wollten wir eigentlich?

Erinnerung Wir suchen randomisierten Primzahl-Test.

Haben wir uns dem genähert?

Erinnerung kleiner Satz von Fermat
 p prim $\Rightarrow \forall a \in \mathbb{Z}_p^*: a^{p-1} \equiv 1 \pmod{p}$

Idee Wähle a zufällig und teste $a^{p-1} \stackrel{?}{\equiv} 1 \pmod{p}$

Der Fermat-Test

Algorithmus 12.23 (Fermat-Test)

1. Wähle $a \in \{2, 3, \dots, p-2\}$ uniform zufällig.
2. If $a \mid p$ Then Ausgabe „ p ist keine Primzahl“; STOP.
3. Berechne $t = a^{p-1} \bmod p$.
4. If $t \neq 1$ Then Ausgabe „ p ist keine Primzahl“; STOP.
5. Ausgabe „ p ist **vielleicht** prim“

bekannt

- Algorithmus korrekt ✓
- Laufzeit polynomiell in $\log p$

Wie groß ist die W'keit, für zusammengesetztes p „vielleicht prim“ auszugeben?

Notation Wir nennen das **Versagensw'keit**.

Ein pessimistischer Blick auf den Fermat-Test

Definition 12.24

$n \in \mathbb{N} \setminus \{1\}$ heißt **Carmichael-Zahl**, wenn n keine Primzahl ist und

$$\forall a \in \mathbb{Z}_n \text{ mit } \text{ggT}(a, n) = 1: a^{n-1} \equiv 1 \pmod{n}$$

gilt.

Beobachtung für Carmichael-Zahlen **Versagensw'keit 1**

Worst-Case-Perspektive Fermat-Test hat **Versagensw'keit 1**

Gibt es überhaupt Carmichael-Zahlen?

Fakten über Carmichael-Zahlen

Fakt $561 = 3 \cdot 11 \cdot 17$ ist eine Carmichael-Zahl.

Fakt 561 ist die kleinste Carmichael-Zahl.

Vielleicht sind Carmichael-Zahlen sehr selten?

Fakt Es gibt 8241 Carmichael-Zahlen $\leq 10^{12}$.

Hoffnung Vielleicht gibt es nur endlich viele Carmichael-Zahlen?

Idee ergänze Fermat-Test um Liste aller Carmichael-Zahlen

leider Es gibt unendlich viele Carmichael-Zahlen.

Ist der Fermat-Test denn für andere Zahlen brauchbar?

Über den Fermat-Test

Theorem 12.27

Sei $n \geq 3$ ungerade und zusammengesetzt, außerdem gebe es ein $a \in \mathbb{Z}_n^*$ mit $a^{n-1} \not\equiv 1 \pmod n$. Der Fermat-Test erkennt n als zusammengesetzt mit W'keit $\geq 1/2$.

Beweis.

Betrachte $L := \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \pmod n\}$

klar $1 \in L$

Beobachtung L abgeschlossen unter $\cdot \pmod n$

denn $(a \cdot b)^{n-1} = a^{n-1} \cdot b^{n-1} \equiv 1 \cdot 1 \pmod n \quad \forall a, b \in L$

also L Untergruppe von \mathbb{Z}_n^*

Erinnerung $L \neq \mathbb{Z}_n^*$ (sonst n Carmichael-Zahl)

klar $|\mathbb{Z}_n^*| \leq n - 2$ **also** $|L| \leq (n - 2)/2$

Erinnerung Wähle $a \in \{2, 3, \dots, n - 2\}$ uniform zufällig.

also **Versagensw'keit** $\leq \frac{|L \setminus \{1, n-1\}|}{|\{2, 3, \dots, n-2\}|} \leq \frac{(n-2)/2-2}{n-3} = \frac{1}{2} \cdot \frac{n-6}{n-3} < \frac{1}{2}$ □ 15

Charakterisierung von Carmichael-Zahlen

Theorem 12.26

Eine zusammengesetzte Zahl $n \in \mathbb{N} \setminus \{1\}$ ist Carmichael-Zahl genau dann, wenn $n - 1$ Vielfaches von $\lambda(n)$ ist.

Beweis.

Beweisrichtung „ \Leftarrow “ Gelte $\lambda(n) \mid (n - 1)$

also $\exists k \in \mathbb{N}: n - 1 = k \cdot \lambda(n)$

Erinnerung $\forall a \in \mathbb{Z}_n: a^{\lambda(n)} \equiv 1 \pmod{n}$

Definition 12.21

also $a^{n-1} = a^{\lambda(n) \cdot k} \equiv 1 \pmod{n}$ ✓

Beweis von Theorem 12.26

zu zeigen n Carmichael-Zahl $\Leftrightarrow \lambda(n) \mid (n - 1)$

Beweisrichtung „ \Rightarrow “ Sei n Carmichael-Zahl

Erinnerung $(a^e \equiv 1 \pmod n) \Leftrightarrow \text{ord}_n(a) \mid e$
Theorem 12.21

klar gilt für alle $a \in \mathbb{Z}_n$

also $(\forall a \in \mathbb{Z}_n : a^e \equiv 1 \pmod n) \Leftrightarrow (\text{kgV} \{ \text{ord}_n(a) \mid a \in \mathbb{Z}_n \} \mid e)$

Erinnerung $\text{kgV} \{ \text{ord}_n(a) \mid a \in \mathbb{Z}_n \} = \lambda(n)$

also mit $e = n - 1$



Zwischenfazit

Wir haben für alle Zahlen **außer** Carmichael-Zahlen
randomisierten Primtest mit Versagensw'keit $\leq 1/2$

klar mit Probability Amplification
Erfolgsw'keit $1 - O\left(\frac{1}{n^k}\right)$ in polynomieller Zeit

jetzt noch mehr Zahlentheorie
für randomisierten Primzahltest für **alle** Zahlen

Das Legendre-Symbol

Definition 12.29

Für $p \geq 3$ prim, $a \in \mathbb{Z}$ ist **Legendre-Symbol** von a und p :

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \in \text{QR}(p) \\ 0 & \text{falls } p \mid a \\ -1 & \text{sonst} \end{cases}$$

Rechenregeln

- $\forall a, b \in \mathbb{Z}: \left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
- $\forall a, b \in \mathbb{Z}$ mit $p \nmid b: \left(\frac{a \cdot b^2}{p}\right) = \left(\frac{a}{p}\right)$
- $\forall a, b \in \mathbb{Z}: \left(\frac{a + b \cdot p}{p}\right) = \left(\frac{a}{p}\right)$
- $\forall a \in \mathbb{Z}: \left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$
- $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

Das Jacobi-Symbol

Erinnerung Legendre-Symbol entspricht Eulerkriterium

jetzt Verallgemeinerung für zusammengesetzte Zahlen

Erinnerung Legendre-Symbol nur für $p \geq 3$ definiert
also nur für ungerade Zahlen verallgemeinern

Definition 12.30

Sei $n \geq 3$ ungerade mit $n = \prod_{i=1}^r p_i$, dabei sei p_i prim für alle $i \in \{1, 2, \dots, r\}$. Für jedes $a \in \mathbb{Z}$ ist

$$\left(\frac{a}{n}\right) := \prod_{i=1}^r \left(\frac{a}{p_i}\right)$$

das **Jacobi-Symbol** von a und n .

Rechenregeln für das Jacobi-Symbol

für $n, m \geq 3$, ungerade, und $a, b \in \mathbb{Z}$

- $\left(\frac{a \cdot b}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$, falls $\text{ggT}(b, n) = 1$
- $\left(\frac{a \cdot b^2}{n}\right) = \left(\frac{a}{n}\right)$, falls $\text{ggT}(b, n) = 1$
- $\left(\frac{a}{n \cdot m}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{a}{m}\right)$, falls $\text{ggT}(a, m) = 1$
- $\left(\frac{a}{n \cdot m^2}\right) = \left(\frac{a}{n}\right)$, falls $\text{ggT}(a, m) = 1$
- $\left(\frac{a+b \cdot n}{n}\right) = \left(\frac{a}{n}\right)$
- $\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right)$
- $\forall k \in \mathbb{N}: \left(\frac{2^{2k} \cdot a}{n}\right) = \left(\frac{a}{n}\right)$
- $\forall k \in \mathbb{N}: \left(\frac{2^{2k+1} \cdot a}{n}\right) = \left(\frac{2}{n}\right) \cdot \left(\frac{a}{n}\right)$
- $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
- $\left(\frac{0}{n}\right) = 0$
- $\left(\frac{1}{n}\right) = 1$

Mehr Rechengesetze für das Jacobi-Symbol

Fakt 12.31 (Quadratisches Reziprozitätsgesetz)

Für ungerade $m, n \geq 1$ gilt:

$$\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{n}{m}\right) & \text{falls } n \equiv 1 \pmod{4} \text{ oder } m \equiv 1 \pmod{4} \\ -\left(\frac{n}{m}\right) & \text{falls } n \equiv 3 \pmod{4} \text{ und } m \equiv 3 \pmod{4} \end{cases}$$

Fakt 12.32

Für ungerades $n \geq 3$ gilt:

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{falls } n \equiv 1 \pmod{8} \text{ oder } n \equiv 7 \pmod{8} \\ -1 & \text{falls } n \equiv 3 \pmod{8} \text{ oder } n \equiv 5 \pmod{8} \end{cases}$$

Berechnung des Jacobi-Symbols

Berechnung von $\left(\frac{a}{n}\right)$ für $a \in \mathbb{Z}$, $n \geq 3$ ungerade
direkt aus den Rechengesetzen

- 1 Falls $a \notin \{1, 2, \dots, n-1\}$, ist das Ergebnis $\left(\frac{a \bmod n}{a}\right)$.
- 2 Falls $a = 0$, ist das Ergebnis 0.
- 3 Falls $a = 1$, ist das Ergebnis 1.
- 4 Falls $4 \mid a$, ist das Ergebnis $\left(\frac{a/4}{n}\right)$.
- 5 Falls $2 \mid a$, unterscheiden wir weiter: Falls $n \bmod 8 \in \{1, 7\}$, ist das Ergebnis $\left(\frac{a/2}{n}\right)$, sonst ist das Ergebnis $-\left(\frac{a/2}{n}\right)$.
- 6 Falls $a \equiv 1 \pmod{4}$ oder $n \equiv 1 \pmod{4}$, ist das Ergebnis $\left(\frac{n \bmod a}{a}\right)$.
- 7 Falls $a \equiv 3 \pmod{4}$ oder $n \equiv 3 \pmod{4}$, ist das Ergebnis $-\left(\frac{n \bmod a}{a}\right)$.

Algorithmus zur Berechnung des Jacobi-Symbols

Algorithmus 12.33

Eingabe ungerades $n \geq 3$, $a \in \mathbb{Z}$

Ausgabe $\left(\frac{a}{n}\right)$

1. $b := a \bmod c$; $c := n$; $s := 1$
2. While $b > 1$
3. While $4 \mid b$
 $b := b/4$
4. If $2 \mid b$ Then
5. If $c \bmod 8 \in \{3, 5\}$ Then $s := -s$
6. $b := b/2$
7. If $b \neq 1$ Then
8. If $(b \bmod 4) = (c \bmod 4) = 3$ Then $s := -s$
9. $(b, c) := (c \bmod b, b)$
10. Ausgabe $s \cdot b$

Über die Berechnung des Jacobi-Symbols

Theorem 12.34

Algorithmus 12.33 berechnen $\left(\frac{a}{n}\right)$ in $O(\log n)$ Durchläufen der While-Schleife (Zeilen 2–9).

Beweis.

zur Korrektheit immer $\left(\frac{a}{n}\right) = s \cdot \left(\frac{b}{c}\right)$

initial $s = 1, b = a \bmod c, c = n$ ✓

induktiv **Annahme** beim Anfang der While-Schleife erfüllt

Beobachtung Zeilen 3–6 entsprechen Rechengesetzen

Beobachtung Zeile 7 sichert, dass bei $b = 1$ nichts mehr passiert

Beobachtung Zeilen 8–9 entsprechen quadratischem Reziprozitätsgesetz ✓

Laufzeit von Alorithmus 12.33

zu zeigen $O(\log n)$ Durchläufe durch While-Schleife

am Ende **immer** ersetze (b, c) durch $(c \bmod b, b)$

Erinnerung entspricht genau euklidischem Algorithmus
(Algorithmus 12.4)

Beobachtung andere Operationen machen b höchstens kleiner

also nicht mehr Durchläufe als beim euklidischen Algorithmus



Der chinesische Restsatz

Theorem 12.35

Seien $m_1, m_2, \dots, m_k \in \mathbb{N}$ mit $\text{ggT}(m_i, m_j) = 1$ für alle $i \neq j$ und $a_1, a_2, \dots, a_k \in \mathbb{N}$. Das Gleichungssystem

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_k \pmod{m_k}$$

hat eine eindeutige Lösung $x \in \left\{ 0, 1, \dots, \left(\prod_{i=1}^k m_i \right) - 1 \right\}$.

Beweis des chinesischen Restsatzes

Definiere $m := \prod_{i=1}^k m_i$, $n_i := m/m_i$

Beobachtung $\text{ggT}(m_i, n_i) = 1$

also $\exists s_i, t_i \in \mathbb{Z}: s_i \cdot m_i + t_i \cdot n_i = 1$

Betrachte $u_i = t_i \cdot n_i$

Beobachtung $u_i = 1 - s_i \cdot m_i \equiv 1 \pmod{m_i}$

Beobachtung $u_i \equiv 0 \pmod{m_j}$ für alle $i \neq j$

also $x = \sum_{i=1}^k a_i \cdot u_i$ ist Lösung

Sei x' andere Lösung

klar $x - x' \equiv 0 \pmod{m_i}$ für alle i

also alle $m_i \mid (x - x')$

Erinnerung $\text{ggT}(m_i, m_j) = 1$ für alle $i \neq j$

zusammen $\left(\prod_{i=1}^k m_i \right) \mid (x - x')$

also x eindeutig in $\left\{ 0, 1, \dots, \left(\prod_{i=1}^k m_i \right) - 1 \right\}$



Über das Jacobi-Symbol

Theorem 12.36

Sei für ungerades $n \geq 3$ die Menge $E(n)$ definiert durch
 $E(n) := \{a \in \mathbb{Z}_n^* \mid a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}\}.$

$$n \text{ prim} \quad \Rightarrow \quad E(n) = \mathbb{Z}_n^*$$

$$n \text{ nicht prim} \quad \Rightarrow \quad |E(n)| \leq |\mathbb{Z}_n^*|/2$$

Beobachtung Theorem 12.36 ist wie Fermat-Test
aber für alle ungeraden Zahlen $n \geq 3$

also Schlüssel für randomisierten Primzahltest

Beweis von Theorem 12.36

Beobachtung $n \geq 3$ ungerade, also $a^{(n-1)/2} \pmod n$ definiert

Beobachtung ebenso $\left(\frac{a}{n}\right)$ definiert

also $E(n)$ definiert

Beweisrichtung n prim $\Rightarrow E(n) = \mathbb{Z}_n^*$

Erinnerung $\forall a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod n$
Definition 12.29, Lemma 12.28

also $E(n) = \mathbb{Z}_n^*$ ✓

Zur anderen Beweisrichtung

zur Beweisrichtung n nicht prim $\Rightarrow |E(n)| \leq |\mathbb{Z}_n^*|/2$

zunächst **nur zeigen** $E(n) \neq \mathbb{Z}_n^*$

Erinnerung $E(n) = \{a \in \mathbb{Z}_n^* \mid a^{(n-1)/2} \equiv 1 \pmod{n}\}$

Annahme $E(n) = \mathbb{Z}_n^*$

dann n jedenfalls Carmichael-Zahl

Behauptung n ungerade und quadratfrei

Erinnerung n ungerade ✓

Annahme n **nicht** quadratfrei

dann $\exists p: p^2 \mid n$

Erinnerung n ungerade, **also** $p > 2$

Erinnerung $p \mid n - 1$ (Theorem 12.26)

also $\exists p > 2: p \mid n$ und $p \mid n - 1$ **Widerspruch**

also $n > 2$ Carmichael-Zahl, ungerade, quadratfrei

Über $E(n)$ für zusammengesetzte n

Wir haben $n > 2$ Carmichael-Zahl, ungerade, quadratfrei

also $\exists p$ prim, $r > 1$: $\text{ggT}(r, p) = 1, n = p \cdot r$

Beobachtung $|\text{QR}(p)| = (p - 1)/2$ (Theorem 12.20)

also $\exists g$: quadratischer Nichtrest modulo p

Betrachte $a \equiv g \pmod{p}, a \equiv 1 \pmod{r}$

Beobachtung Lösung a existiert (chinesischer Restsatz)

Beobachtung $a \in \mathbb{Z}_n^*$, weil $\text{ggT}(a, n) = 1$

Erinnerung **Annahme** $E(n) = \mathbb{Z}_n^*$

dann $a \in E(n)$

mit Rechenregeln
$$\begin{aligned} \left(\frac{a}{n}\right) &= \left(\frac{a}{p \cdot r}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{r}\right) = \left(\frac{g}{p}\right) \cdot \left(\frac{1}{r}\right) \\ &= (-1) \cdot 1 = -1 \end{aligned}$$

Über $E(n)$ für zusammengesetzte n (Fortsetzung)

Wir haben $a^{(n-1)/2} \equiv 1 \pmod r$

Erinnerung $a^{(n-1)/2} \equiv 1 \pmod n$ oder $a^{(n-1)/2} \equiv -1 \pmod n$
(Lemma 12.28)

also $a^{(n-1)/2} \equiv 1 \pmod n$
weil $n = p \cdot r$ mit p prim und $r > 2$

also $a^{(n-1)/2} \pmod n \neq \left(\frac{a}{n}\right)$

also $a \notin E(n)$ **Widerspruch**

also $E(n) \neq \mathbb{Z}_n^*$ ✓

Beweis von Theorem 12.36

Wir haben n zusammengesetzt $\Leftrightarrow E(n) \neq \mathbb{Z}_n^*$

zu zeigen $E(n) \neq \mathbb{Z}_n^* \Rightarrow |E(n)| \leq |\mathbb{Z}_n^*| / 2$

dazu ausreichend $E(n)$ ist Untergruppe

klar $1 \in E(n)$

Betrachte $x \cdot y$ für $x, y \in E(n)$

Erinnerung $x^{(n-1)/2} \equiv \left(\frac{x}{n}\right) \pmod n, y^{(n-1)/2} \equiv \left(\frac{y}{n}\right) \pmod n$

also $(x \cdot y)^{(n-1)/2} = x^{(n-1)/2} \cdot y^{(n-1)/2} \equiv \left(\frac{x}{n}\right) \cdot \left(\frac{y}{n}\right) \pmod n$

Erinnerung $\left(\frac{x}{n}\right) \cdot \left(\frac{y}{n}\right) = \left(\frac{x \cdot y}{n}\right)$



Primzahltest von Solovay und Strassen

Algorithmus 12.37

Eingabe $n \in \mathbb{N} \setminus \{1\}, k \in \mathbb{N}$

1. If $n = 2$ Then Ausgabe „ n ist prim“; STOP.
2. If n gerade Then Ausgabe „ n ist zusammengesetzt“; STOP.
3. While $k \geq 1$
 4. Wähle $a \in \{2, 3, \dots, n - 1\}$ uniform zufällig.
 5. Berechne $d := \text{ggT}(a, n)$.
 6. If $d \neq 1$ Then Ausgabe „ n ist zusammengesetzt“; STOP.
 7. Berechne $b \equiv a^{(n-1)/2} \pmod n$.
 8. If $b \notin \{-1, 1\} \pmod n$ Then
Ausgabe „ n ist zusammengesetzt“; STOP.
 9. Berechne $c := \left(\frac{a}{n}\right)$.
 10. If $b \not\equiv c \pmod n$ Then Ausgabe „ n ist zusammengesetzt“; STOP.
 11. $k := k - 1$
12. Ausgabe „ n ist vermutlich prim“

Über den Algorithmus von Strassen

Theorem 12.38

Für den Algorithmus von Solovay und Strassen (Algorithmus 12.37) gelten bei Eingabe von $n \in \mathbb{N} \setminus \{1, 2\}$ und $k \in \mathbb{N}$ die folgenden Aussagen.

- 1 Die Rechenzeit beträgt $O(k \cdot \log n)$.
- 2 Für Primzahlen n wird „ n ist vermutlich prim“ ausgegeben.
- 3 Für zusammengesetzte n wird mit Wahrscheinlichkeit mindestens $1 - 2^{-k}$ „ n ist zusammengesetzt“ ausgegeben.

Beweis.

- 1 schon gezeigt jede Zeile in Zeit $O(\log n)$
klar genau k While-Schleife-Durchläufe
also Gesamtrechenzeit $O(k \cdot \log n)$ ✓

Beweis der Korrektheit für Primzahlen

② **Beobachtung** Ausgabe „ n ist zusammengesetzt“ nur, wenn

- n gerade (für Primzahlen $n > 2$ nicht möglich) ✓
- $\text{ggT}(a, n) \neq 1$ (für Primzahlen nicht möglich) ✓
- $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$ (für Primzahlen $n > 2$ und $a \in \mathbb{Z}_n^*$ nicht möglich) ✓

also immer Ausgabe „ n ist vermutlich prim“ ✓

③ **Beobachtung** genügt zu zeigen in einem While-Schleifen-Durchgang Ausgabe „ n ist zusammengesetzt“ mit W'keit $\geq 1/2$

dann Rest mit Probability Amplification

Über eine Runde mit zusammengesetztem n

Beobachtung falls n gerade,
richtige Ausgabe mit W'keit 1 ✓

Beobachtung falls $\text{ggT}(a, n) \neq 1$,
richtige Ausgabe mit W'keit 1 ✓

also ab jetzt n ungerade und $\text{ggT}(a, n) = 1$

also Theorem 12.36 anwendbar
also richtige Ausgabe mit W'keit $\geq 1/2$ □

Eine Hilfsaussage zur Dechiffrierung

Lemma 12.39

Für alle Primzahlen p und alle $a, k \in \mathbb{N}_0$ gilt $a^{1+k \cdot (p-1)} \equiv a \pmod{p}$.

Beweis.

1. Fall $a \equiv 0 \pmod{p}$ ✓

2. Fall $a \not\equiv 0 \pmod{p}$

also $\text{ggT}(a, p) = 1$

Beobachtung $a^{1+k \cdot (p-1)} \equiv a \cdot (a^{p-1})^k \pmod{p}$

also $a^{p-1} \equiv 1 \pmod{p}$
kleiner Satz von Fermat

also $a^{1+k \cdot (p-1)} \equiv a \pmod{p}$ □

Korrektheit der Dechiffrierung bei RSA

Wir haben $(m^e)^d = m^{1+t \cdot (p-1) \cdot (q-1)}$

mit Lemma 12.39 $(m^e)^d \equiv m \pmod{p}$
und $(m^e)^d \equiv m \pmod{q}$

Beobachtung genau ein $x \in \{0, 1, \dots, p \cdot q - 1\}$ erfüllt das chinesischer Restsatz

Beobachtung m erfüllt das

also m eindeutige Lösung der Dechiffrierung ✓