



*Problema, numeros primos a compositis dignoscendi ... ad gravissima ac utilissima tabus arithmeticae pertinere...
... scientiae dignitas requirere videtur, ut omnia subsidia ad solutionem problematis tam elegantis ac celeberrimi sedulo excolantur.*

J. C. F. GAUSS (1777–1855),
Disquisitiones Arithmeticae, Artikel 329

- ▶ Probedivision: n ist Primzahl $\Leftrightarrow \forall_{k: 2 \leq k \leq \sqrt{n}} k \nmid n$

```

IS_PRIME (int n)
{
    for (int i = 2; i <= sqrt(n); i++)
        if (i | n) return FALSE;
    return TRUE;
}
    
```

- ▶ logarithmisches Kostenmodell:

- ▶ input-Grösse ist $\log n$
- ▶ Anzahl der Schleifendurchläufe ist $O(\sqrt{n}) = O(2^{\frac{1}{2} \log n})$
- ▶ Jede Probedivision erfordert $O(\log^2 n)$ Bit-Operationen
- ▶ Laufzeit für m -stelliges n ist im worst-case $O(m^2 \cdot 2^{m/2})$

Pseudo-Primzahltests

- ▶ $A(n, a)$: Eigenschaft ganzer Zahlen mit

$$n \text{ Primzahl} \Rightarrow \forall_{a: 1 < a < n} A(n, a)$$

- ▶ Wird w ($1 < w < n$) gefunden mit $\neg A(n, w)$, so ist n keine Primzahl:

$$\exists_{w: 1 < w < n} \neg A(n, w) \Rightarrow n \text{ ist keine Primzahl}$$

- ▶ Solch ein w heisst Zeuge (witness) für die Zusammengesetztheit von n

- ▶ Beispiele

- ▶ Teilbarkeitstest

$$D(n, a) : a \nmid n$$

- ▶ Euklid-Test

$$E(n, a) : \text{ggT}(n, a) = 1$$

- ▶ Fermat-Test

$$F(n, a) : \text{ggT}(n, a) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$$

- ▶ SPP-Test ("strong probable prime", MILLER-RABIN)

sei $n - 1 = 2^t \cdot u$ mit ungeradem u

$$MR(n, a) : \begin{cases} a^u \equiv 1 \pmod{n} & \text{oder} \\ a^{u \cdot 2^i} \equiv -1 \pmod{n} & \text{für ein } i \text{ mit } 0 \leq i < t \end{cases}$$

► Begründung für den SPP-Test

$$MR(n, a) : n - 1 = 2^t \cdot u \text{ mit ungeradem } u$$

$$\begin{cases} a^u \equiv 1 \pmod{n} & \text{oder} \\ a^{u \cdot 2^i} \equiv -1 \pmod{n} & \text{für ein } i \text{ mit } 0 \leq i < t \end{cases}$$

- n Primzahl $\Leftrightarrow \mathbb{Z}_n$ Körper
- In einem Körper hat die Gleichung $x^2 = 1$ genau zwei Lösungen $x = \pm 1$
(allgemeiner: $x^2 = 1$ hat für $n = p^e$ ($p \geq 3$ Primzahl) in \mathbb{Z}_n genau die beiden Lösungen $x = \pm 1$)
- wird in \mathbb{Z}_n^* ein Element $z \neq \pm 1$ mit $z^2 = 1$ gefunden, so ist n keine Primzahl
- beachte sukzessive Quadrierungen in \mathbb{Z}_n^*

$$a^u \pmod{n}, a^{2u} \pmod{n}, a^{2^2 u} \pmod{n}, a^{2^3 u} \pmod{n}, \dots, a^{2^t u} \pmod{n}$$



Beispiele

- $n = 25, n - 1 = 3 \cdot 8, a = 7:$

$$7^3 \equiv 18 \pmod{25}$$

$$7^6 \equiv 24 \pmod{25}$$

$$7^{12} \equiv 1 \pmod{25}$$

$$7^{24} \equiv 1 \pmod{25}$$

Test bringt keine Information! $a = 7$ ist kein MR-Zeuge.



- $n = 25, n - 1 = 3 \cdot 8, a = 2:$

$$2^3 \equiv 8 \pmod{25}$$

$$2^6 \equiv 14 \pmod{25}$$

$$2^{12} \equiv 21 \pmod{25}$$

$$2^{24} \equiv 16 \pmod{25}$$

Test zeigt, daß 25 nicht prim ist! $a = 2$ ist MR-Zeuge.



- $n = 2047 = 23 \cdot 89, n - 1 = 2 \cdot 1023, a = 2:$

$$2^{1023} \equiv 1 \pmod{2047}$$

$$2^{2046} \equiv 1 \pmod{2047}$$

Test bringt keine Information! $a = 2$ ist kein MR-Zeuge.



- $n = 2047 = 23 \cdot 89, n - 1 = 2 \cdot 1023, a = 3$:

$$3^{1023} \equiv 1565 \pmod{2047}$$

$$3^{2046} \equiv 1013 \pmod{2047}$$

Test zeigt, daß 2047 nicht prim ist! $a = 3$ ist MR-Zeuge.

- $n = 341 = 11 \cdot 31, n - 1 = 4 \cdot 85, a = 2$

$$2^{85} \equiv 32 \pmod{341}$$

$$2^{170} \equiv 1 \pmod{341}$$

$$2^{340} \equiv 1 \pmod{341}$$

Test zeigt, daß 341 nicht prim ist! $a = 2$ ist MR-Zeuge.



- $n = 561 = 3 \cdot 11 \cdot 17, n - 1 = 16 \cdot 35, b = 2$

$$2^{35} \equiv 263 \pmod{561}$$

$$2^{70} \equiv 166 \pmod{561}$$

$$2^{140} \equiv 67 \pmod{561}$$

$$2^{280} \equiv 1 \pmod{561}$$

$$2^{560} \equiv 1 \pmod{561}$$

Test zeigt, daß 561 nicht prim ist! $b = 2$ ist MR-Zeuge.

In der Tat ist 561 die kleinste CARMICHAEL-Zahl, also eine Zahl, bei der es ausser den GGT-Zeugen keine weiteren FERMAT-Zeugen gibt! Man weiss erst seit 1994, dass es unendlich-viele solche Zahlen gibt

(ALFORD, W.R.; GRANVILLE, A.; AND POMERANCE, C).

Siehe:

<http://mathworld.wolfram.com/CarmichaelNumber.html>

- $n = 2243, n - 1 = 2 \cdot 1121, b = 2$

$$2^{1121} \equiv 2242 \pmod{2243}$$

$$2^{2242} \equiv 1 \pmod{2243}$$

$b = 2$ ist kein MR-Zeuge für die Zusammengesetztheit von 2243. Solche Zeugen darf und kann es nicht geben, denn 2243 ist Primzahl!



Beispiele für Zeugenmengen:

► $n = 13$

$$\begin{aligned} Dzeugen(13) &= [] \\ Ezeugen(13) &= [] \\ Fzeugen(13) &= [] \\ MRzeugen(13) &= [] \end{aligned}$$

► $n = 14$

$$\begin{aligned} Dzeugen(14) &= [2, 7] \\ Ezeugen(14) &= [2, 4, 6, 7, 8, 10, 12] \\ Fzeugen(14) &= [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13] \\ MRzeugen(14) &= [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13] \end{aligned}$$



► $n = 15$

$$\begin{aligned} Dzeugen(15) &= [3, 5] \\ Ezeugen(15) &= [3, 5, 6, 9, 10, 12] \\ Fzeugen(15) &= [2, 3, 5, 6, 7, 8, 9, 10, 12, 13] \\ MRzeugen(15) &= [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13] \end{aligned}$$

► $n = 25$

$$\begin{aligned} Dzeugen(25) &= [5] \\ Ezeugen(25) &= [5, 10, 15, 20] \\ Fzeugen(25) &= [2, \dots, 6, 8, \dots, 17, 20, \dots, 23] \\ MRzeugen(25) &= [2, \dots, 6, 8, \dots, 17, 20, \dots, 23] \end{aligned}$$



Vergleich der Grösse von Zeugenmengen

n	D	E	F	MR
2	0	0	0	0
3	0	0	0	0
4	1	1	2	2
5	0	0	0	0
6	2	3	4	4
7	0	0	0	0
8	2	3	6	6
9	1	2	6	6
10	2	5	8	8
12	4	7	10	10
14	2	7	12	12
15	2	6	10	12



Vergleich der Grösse von Zeugenmengen

n	D	E	F	MR
16	3	7	14	14
18	4	11	16	16
20	4	11	18	18
21	2	8	16	18
22	2	11	20	20
24	6	15	22	22
25	1	4	20	20
26	2	13	24	24
27	2	8	24	24
28	4	15	24	24



Vergleich der Grösse von Zeugenmengen

n	D	E	F	MR
30	6	21	28	28
⋮	⋮	⋮	⋮	⋮
105	6	56	88	102
⋮	⋮	⋮	⋮	⋮
169	1	12	156	156
⋮	⋮	⋮	⋮	⋮
561	6	240	240	550
⋮	⋮	⋮	⋮	⋮
1105	6	336	336	1074
⋮	⋮	⋮	⋮	⋮
1729	6	432	432	1566
⋮	⋮	⋮	⋮	⋮



► Idee (probabilistischer) Primzahltests:

Gelingt es trotz intensiver (zufälliger) Bemühungen nicht, einen Zeugen für die Zusammengesetztheit von n aufzutreiben, wird man n für eine Primzahl halten

► Annahme:

- für n, a mit $1 < a < n$ ist die Un/Gültigkeit von $A(n, a)$ leicht zu überprüfen
- ist n keine Primzahl, so sind Zeugen für die Zusammengesetztheit von n häufig



► Probabilistisches Verfahren:

- ▶ wähle zufällig Kandidaten k_1, k_2, \dots, k_r mit $1 < k_i < n$ und überprüfe $A(n, k_i) (1 \leq i \leq r)$
- ▶ wird dabei mindestens ein Zeuge für die Zusammengesetztheit von n gefunden, d.h. $\neg A(n, k_i)$, so ist n in der Tat zusammengesetzt
— diese Aussage ist korrekt!
- ▶ wird kein Zeuge für die Zusammengesetztheit von n gefunden, so wird n als Primzahl deklariert
— dies ist mit nur sehr geringer Wahrscheinlichkeit eine falsche Entscheidung

Diskussion der Tests:

- ▶ Teilbarkeitstest
Unbrauchbar, da es Nicht-Primzahlen n mit nur zwei Teilern ($\neq 1, n$) gibt (Teilbarkeits-Zeugen)
- ▶ Euklid-Test
Unbrauchbar, da es Nicht-Primzahlen n mit nur wenigen Euklid-Zeugen gibt
- ▶ Fermat-Test
Unbrauchbar, da es zusammengesetzte Zahlen n gibt mit

$$\forall_{1 < a < n} : \text{ggT}(n, a) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$$

d.h. alle Fermat-Zeugen sind schon Euklid-Zeugen

► Der Primzahltest von Miller-Rabin:

- ▶ wähle (iteriert und zufällig) Zahlen

$$a \in \mathbb{Z}_n, a \neq \{0, 1\} \text{ mit } \text{ggT}(n, a) = 1$$

(falls a mit $\text{ggT}(n, a) \neq 1$: sowieso fertig)

- ▶ berechne $a^{n-1} \pmod n$ durch "schnelle Exponentiation", d.h. durch iteriertes Quadrieren und Multiplizieren:

$$a^{(n-1) \text{ div } 2^j} \text{ für } j = k, k-1, k-2, \dots, 1, 0,$$

wobei $k = \ell(n-1) + 1$

- ▶ falls auf diesem Weg eine Situation

$$z \mapsto z^2 = 1 \text{ mit } z \neq \pm 1$$

angetroffen wird: Zeuge für Zusammengesetztheit von n gefunden!

```

Miller_Rabin (int n)
{
  choose a ∈ [2 : n - 1] at random;
  /* primes are odd except for 2, which is an odd prime :-*) */
  if (n == 2) return TRUE;
  if (n == 1 || even(n)) return FALSE;
  /* primes are relatively prime to a */
  if (ggT(a, n) > 1) return FALSE;
  /* compute z = a^{n-1} ≠ 1 mod n using iterated squaring */
  let (b_k, ..., b_0) be the binary representation of n - 1;
  int z = 1;
  for (int i = k; i ≥ 0; i--)
  {
    int x = z;
    z = z^2 mod n;
    /* primes allow only trivial solutions of x^2 ≡ 1 mod p */
    if ((z == 1) && (x ≠ 1) && (x ≠ n - 1)) return FALSE;
    if (b_i == 1) z = z · a mod n;
  }
  if (z ≠ 1 mod n) return FALSE; /* z = a^{n-1} */
  return TRUE; /* no witness found: in dubio pro reo */
}
    
```

Beachte:

- ▶ ist $n - 1 = 2^t \cdot u$ mit ungeradem u , so
 - ▶ sind die letzten $t + 1$ Werte von z beim Quadrieren und Multiplizieren

$$a^u \bmod n, a^{2^1 u} \bmod n, a^{2^2 u} \bmod n, a^{2^3 u} \bmod n, \dots, a^{2^{t-1} u} \bmod n$$

- ▶ sind die letzten t Operationen sind nur Quadrierungen

- ▶ *der einfache Fall:*

es gibt in \mathbb{Z}_n^* einen Fermat-Zeugen,
d.h. ein $a \in \mathbb{Z}_n^*$ mit $a^{n-1} \not\equiv 1 \pmod n$

- ▶ $B = \{b \in \mathbb{Z}_n^*; b^{n-1} \equiv 1 \pmod n\}$ ist eine Untergruppe von \mathbb{Z}_n^*
- ▶ alle Nicht-Zeugen gehören zu B
- ▶ wegen $x \notin B$ ist B eine echte Untergruppe von \mathbb{Z}_n^*

Lemma:

- ▶ *Miller-Rabin-Zeugen sind häufig,
genauer:
ist n eine zusammengesetzte Zahl, so ist die Anzahl der Miller-Rabin-Zeugen für diese Tatsache mindestens $(n - 1)/2$*

zu diesem Zweck wird gezeigt:

- ▶ Nicht-Zeugen sind Elemente von \mathbb{Z}_n^* (klar!)
- ▶ Die Nicht-Zeugen bilden eine echte Untergruppe von \mathbb{Z}_n^*
- ▶ Wegen des Satzes von Lagrange hat diese Untergruppe $\leq \#\mathbb{Z}_n^*/2 \leq (n - 1)/2$ Elemente
- ▶ es gilt sogar (Beweis etwas aufwendiger):
die Untergruppe der Nicht-Zeugen hat $\leq \varphi(n)/4$ Elemente

- ▶ *der etwas weniger einfache Fall:*

es gibt in \mathbb{Z}_n^* keine Fermat-Zeugen,
d.h. $a^{n-1} \equiv 1 \pmod n$ für alle $a \in \mathbb{Z}_n^*$

- ▶ *der einfache Unter-Fall des etwas weniger einfachen Falles:*

$n = p^e$ mit Primzahl $p > 2$ und $e > 2$

- ▶ Fakt: $\mathbb{Z}_{p^e}^*$ ist eine zyklische Gruppe
- ▶ $\#\mathbb{Z}_{p^e}^* = \varphi(p^e) = p^{e-1}(p - 1)$
- ▶ Ist $a \in \mathbb{Z}_{p^e}^*$ ein Element der Ordnung $\varphi(p^e)$, so gilt $a^{\varphi(p^e)} \equiv 1 \pmod n$ und $a^{n-1} \equiv 1 \pmod n$, also $\varphi(p^e) = p^{e-1}(p - 1) \mid p^e - 1$: unmöglich!

- ▶ der etwas weniger einfache Unter-Fall des etwas weniger einfachen Falles:

$$n = n_1 \cdot n_2 \text{ mit } n_1, n_2 > 1 \text{ und } \text{ggT}(n_1, n_2) = 1$$

- ▶ $n - 1 = 2^t \cdot u$ mit ungeradem u , für $a \in \mathbb{Z}_n^*$ betrachte

$$[a] = \langle a^u \bmod n, a^{2u} \bmod n, a^{2^2 u} \bmod n, a^{2^3 u} \bmod n, \dots, a^{2^t u} \bmod n \rangle$$

- ▶ beachte: die letzte Komponente von $[a]$ ist immer = 1;
- ▶ sei j mit $0 \leq j < t$ maximal mit der Eigenschaft, dass es ein $v \in \mathbb{Z}_n^*$ gibt $v^{2^j u} \equiv -1 \pmod n$



- ▶ $B = \{x \in \mathbb{Z}_n^*; x^{2^j u} \equiv \pm 1 \pmod n\} \neq \emptyset$
- ▶ B ist eine Untergruppe von \mathbb{Z}_n^* , die alle Nicht-Zeugen enthält
- ▶ B ist eine echte Untergruppe von \mathbb{Z}_n^* :
 - sei $v \in \mathbb{Z}_n^*$ mit $v^{2^j u} \equiv -1 \pmod n$
 - $\Rightarrow v^{2^j u} \equiv -1 \pmod{n_1}$ und $v^{2^j u} \equiv -1 \pmod{n_2}$
 - Konstruiere mittels Chinesischem Restesatz $w \in \mathbb{Z}_n^*$ mit $w \equiv v \pmod{n_1}$ und $w \equiv 1 \pmod{n_2}$
 - $\Rightarrow w^{2^j u} \equiv -1 \pmod{n_1}$ und $w^{2^j u} \equiv 1 \pmod{n_2} \Rightarrow w \notin B$



Theorem (MILLER, RABIN, 1976)

- ▶ Der Miller-Rabin-Primzahltest beurteilt bei m Iterationen eine zusammengesetzte Zahl n fälschlicherweise als Primzahl mit einer Wahrscheinlichkeit $< (1/2)^m$ bei einer Laufzeit von $\mathcal{O}(m \cdot \ell(n)^3)$

In der Terminologie der Komplexitätstheorie

$$\text{PRIMES} \in \text{co-RP}$$

wobei: $\text{RP} = \text{random polynomial time}$
 = Klasse der Probleme mit effizienten probabilistischen Entscheidungsverfahren mit einseitigem Fehler ("biased Monte Carlo")



▶ Zahlenbeispiel zur Effizienz des MILLER-RABIN-Tests:

- ▶ ε : Fehlerwahrscheinlichkeit des MR-Tests
- ▶ Aufwand zum Testen einer k -stelligen Zahl $(\log \frac{1}{\varepsilon} \cdot k^3)$
- ▶ Annahme:
 10^6 arithmetische Operationen pro Sekunde, $\varepsilon = 10^{-100}$

$$\begin{aligned} k = 30 &\Rightarrow 1 \text{ sec} \\ k = 50 &\Rightarrow 12.5 \text{ sec} \\ k = 100 &\Rightarrow 100 \text{ sec} \end{aligned}$$



Ein wesentlich schwieriger darzustellendes und zu begründendes Verfahren von ADLEMAN und HUANG (1992) zeigt

$$\text{PRIMES} \in \text{RP}$$

Aus beiden Aussagen zusammen erhält man

$$\text{PRIMES} \in \text{ZPP} = \text{RP} \cap \text{co-RP}$$

wobei: $\text{ZPP} = \text{zero error random polynomial time}$
 = Klasse der Probleme mit probabilistischen Entscheidungsverfahren, die im Mittel effizient sind
 ("Las Vegas")

Weitere Informationen zur Komplexitätssituation für PRIMES

- ▶ Primzahlen sind effizient verifizierbar (PRATT, 1975)

$$\text{PRIMES} \in \text{NP}$$

- ▶ Zusammen mit dem offensichtlichen (!!)
- $\text{PRIMES} \in \text{co-NP}$ ergibt sich

$$\text{PRIMES} \in \text{NP} \cap \text{co-NP}$$

- ▶ MILLER hat 1976 gezeigt, dass Primzahlen *deterministisch* mit Aufwand $\mathcal{O}(\log^5 n)$ erkannt werden können, denn
 - ▶ ist n keine Primzahl, dann ist kleinste MR-Zeuge für die Zusammengesetztheit von n kleiner als $2 \ln^2 n$ (BACH, 1985)
 Hierbei wird allerdings eine bislang unbewiesene Hypothese des Zahlentheorie (ERH) verwendet!
- ▶ Es gibt einen (in der Praxis!!) sehr effizienten *deterministischen* Primzahltest von ADELMAN, POMERANCE, RUMELEY (1983) mit Laufzeit

$$\mathcal{O}((\log n)^{c \cdot \log \log \log n})$$

- ▶ Im August 2002 wurde von AGRAWAL, KAYAL, SAXENA das lange offene Problem endlich gelöst:

$$\text{PRIMES} \in \mathbb{P}$$

- ▶ Literaturhinweise:

- ▶ R. CRANDALL, C. POMERANCE, *Prime Numbers, A Computational Perspective*, Springer-Verlag, 2001.
- ▶ M. DIETZFELBINGER, *Primality Testing in Polynomial Time*, Springer Verlag 2004.
- ▶ siehe auch Webseite zur Vorlesung