

Die Primheit von Primzahlen kann man effizient  
*verifizieren*

oder

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



*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 celebris sedulo excolantur.*

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



► Die Zahl

$n = 114381625757888867669235779976146612010218296721242$   
 $362562561842935706935245733897830597123563958705$   
 $058989075147599290026879543541$

ist *keine* Primzahl.

► Klar! Denn  $n = p \cdot q$  mit

$p = 34905295108476509491478496199038981334177646384933$   
 $87843990820577$

$q = 32769132993266709549961988190834461413177642967992$   
 $942539798288533$

►  $p$  und  $q$  sind Primzahlen! Aber wie garantiert man das?

►  $n$  ist Kryptologen bekannt als RSA-129.



aus der Übersetzung von MASER (1889):

*Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten als auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. [. . .] ausserdem dürfte es die Würde der Wissenschaft erheischen, alle Hilfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommen.*

*Trotzdem muss man gestehen, dass alle bisher angegebenen Methoden entweder auf sehr spezielle Fälle beschränkt oder so mühsam und weitläufig sind, dass sie [. . .] auf grössere Zahlen aber meistens kaum angewendet werden können.*



K. GÖDEL (Brief an J. VON NEUMANN, 1956)

Wenn es eine Maschine mit ... gäbe, hätte das Folgerungen von der grössten Tragweite. Es würde offenbar bedeuten, dass man trotz der Unlösbarkeit des Entscheidungsproblems die Denkarbeit der Mathematiker bei ja-oder-nein-Fragen vollständig (abgesehen von der Aufstellung der Axiome) durch Maschinen ersetzen könnte.

... bedeutet, dass die Anzahl der Schritte gegenüber dem blossen Probieren von  $N$  auf  $\log N$  verringert werden kann. So starke Verringerungen kommen aber bei anderen finiten Problemen durchaus vor, z.B. bei der Berechnung eines quadratischen Restsymbols durch wiederholte Anwendung des Reziprozitätsgesetzes. Es wäre interessant zu wissen, wie es damit z.B. bei der Feststellung, ob eine Zahl Primzahl ist, steht und wie stark im allgemeinen bei finiten kombinatorischen Problemen die Anzahl der Schritte gegenüber dem blossen Probieren verringert werden kann.

## Primzahltest mittels Probekdivision

► Kriterium:

$$n \text{ ist Primzahl} \Leftrightarrow \forall a: 2 \leq a \leq \sqrt{n} \ a \nmid n$$

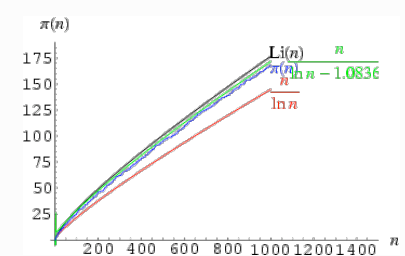
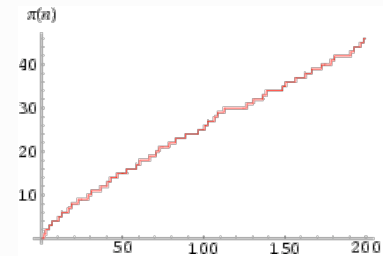
► Logarithmisches Kostenmodell:

- Input-Grösse ist  $\log n$
- Anzahl der Probekdivisionen:  $O(\sqrt{n}) = O(2^{\frac{1}{2} \log n})$
- Jede Probekdivision erfordert  $O(\log^2 n)$  Bit-Operationen
- Laufzeit für  $m$ -stelliges  $n$  ist im worst-case  $O(m^2 \cdot 2^{m/2})$
- Exponentieller Aufwand in Problemgrösse  $m = \log n$  — prohibitiv!
- NB: man kann sich bei den Probekteilern  $a$  auf Primzahlen beschränken.

## Häufigkeit von Primzahlen

- Primzahlsatz (von GAUSS vermutet, erst viel später von HADAMARD und DE LA VALLÉE-POUSSIN bewiesen)

$$\pi(n) = \#\{p \leq n; p \text{ Primzahl}\} \sim \frac{n}{\ln n}$$



Konkreter:

- Das Testen einer Zahl  $n \sim 10^k$  erfordert etwa  $\frac{10^{k/2}}{(k/2) \log 10}$  Probekdivisionen
- Annahme: man kann pro Sekunde  $10^6$  Divisionen ausführen.
- Dann benötigt ein Primzahltest per Probekdivision für eine Zahl mit  $k$  Dezimalstellen etwa

$$\frac{10^{k/2}}{(k/2) \log 10 \times 10^6 \times 60 \times 60 \times 24 \times 365} = \frac{10^{k/2}}{k} \times 2.75 \times 10^{-14} \text{ Jahre}$$

► Einige Zahlenbeispiele:

$$\begin{aligned} k=30 &\Rightarrow 11 \text{ Monate} \\ k=50 &\Rightarrow 5.5 \times 10^9 \text{ Jahre} \\ k=100 &\Rightarrow 2.75 \times 10^{34} \text{ Jahre} \end{aligned}$$

## Entscheidung versus Verifikation

► Beispiele:

$$2^{67} - 1 \in \text{PRIM} ? \quad 2^{128} + 1 \in \text{PRIM} ? \quad 2^{858433} - 1 \in \text{PRIM} ?$$

► Zusammengesetztheit hat effiziente Zeugen (z.B. Teiler)

$$\begin{aligned} 2^{67} - 1 &= 147.573.952.589.676.412.927 \\ &= 761.838.257.287 \cdot 193.707.721 \end{aligned}$$

[Frank COLE (1903) benötigte “die Sonntage dreier Jahre” ...]

Es ginge in diesem Fall auch (FERMAT)

$$3^{2^{67}-2} \pmod{2^{67} - 1} = 95.591.506.202.441.271.281$$

aber das geht nicht immer!



► Wie kann man jemanden effizient davon überzeugen, dass eine vorgelegte (sehr grosse) Zahl  $N$  keine Primzahl ist?

- Man nimmt zwei geeignete Zahlen  $P, Q$ , multipliziert sie und überprüft:

$$N \stackrel{?}{=} P \times Q$$

- Teiler einer Zahl sind “Zeugen” dafür, dass die Zahl nicht Primzahl ist.
- Analog kann man ggT-Berechnungen verwenden.
- Es wird nicht verlangt, dass Zeugen leicht zu finden sind!
- Fazit: Nicht-Primzahlen lassen sich effizient verifizieren!



## Körper und Ordnungen

► Wie kann man jemanden effizient davon überzeugen, dass eine vorgelegte (sehr grosse) Zahl  $N$  eine Primzahl ist?

Gibt es “Zeugen” dafür, dass eine Zahl keine echten Teiler besitzt?

Lassen sich Primzahlen effizient verifizieren?

- Ja! Aber das ist keineswegs offensichtlich (PRATT, 1975).

► Grundsätzliche Bemerkung:

Per def. ist Primheit eine “universelle” und Nicht-Primheit eine “existentielle” Eigenschaft von Zahlen.

►  $\mathbb{F}$  Körper,  $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$  : multiplikative Gruppe

► Fakt: In einem Körper  $\mathbb{F}$  hat ein Polynom vom Grad  $k$  höchstens  $k$  Nullstellen (Vielfachheiten mitgezählt)

► Für  $a \in \mathbb{F}^*$  :  $\text{ord}_{\mathbb{F}^*}(a)$  Ordnung von  $a$  in  $\mathbb{F}^*$

$$\text{ord}_{\mathbb{F}^*}(a) = \# \langle a \rangle = \min \{ t \geq 1 ; a^t = 1 \}$$

► Für  $a \in \mathbb{F}^*, n \geq 1$ :

$$\text{ord}_{\mathbb{F}^*}(a) \mid n \Leftrightarrow a \text{ ist Nullstelle von } X^n - 1$$

► Folgerung: In einem Körper  $\mathbb{F}$  gibt es höchstens  $n$  Elemente  $a \in \mathbb{F}$  mit  $\text{ord}_{\mathbb{F}^*}(a) \mid n$  ( $n \geq 1$ ).



► Lemma: Für  $n \geq 1$  ist die Anzahl der Elemente  $a \in \mathbb{F}$  mit  $ord_{\mathbb{F}^*}(a) = n$  entweder  $= 0$  oder  $= \varphi(n)$ .

► Beweis: sei  $a \in \mathbb{F}^*$  mit  $ord_{\mathbb{F}^*}(a) = n$ .  
Für  $a^k \in \langle a \rangle$   $k \in \mathbb{Z}_n$  gilt  $(a^k)^n = (a^n)^k = 1^k = 1$ ,  
dies sind genau  $n$  verschiedene Nullstellen von  $X^n - 1$ .  
Weitere kann es nicht geben. Es gilt

$$ord_{\mathbb{F}^*}(a^k) = \frac{n}{\text{ggT}(k, n)},$$

$$ord_{\mathbb{F}^*}(a^k) = n \text{ für } k \in \mathbb{Z}_n^*.$$



- Folgerung:  $\mathbb{F}$  endlicher Körper  $\Rightarrow \mathbb{F}^*$  zyklische Gruppe.
- Die  $a \in \mathbb{F}^*$  mit  $\langle a \rangle = \mathbb{F}^*$  nennt man *primitive Elemente* von  $\mathbb{F}$ .
- Es ist nicht klar, wie man primitive Elemente tatsächlich findet — ausser durch Probieren....



► Satz: Jede *endliche* Untergruppe  $G$  von  $\mathbb{F}^*$  ist zyklisch.

► Beweis: Sei  $\#G = n$ , also (LAGRANGE!)  $ord_{\mathbb{F}^*}(a) \mid n$  für alle  $a \in G$ . Für  $d \mid n$  sei

$$\chi(d) = \begin{cases} 1 & \text{es gibt ein } a \in G \text{ mit } ord_{\mathbb{F}^*}(a) = d \\ 0 & \text{sonst} \end{cases}$$

Dann ist

$$n = \sum_{d \mid n} \chi(d) \cdot \varphi(d) \leq \sum_{d \mid n} \varphi(d) = n$$

Also gilt Gleichheit und somit  $\chi(d) = 1$  für alle  $d \mid n$ .  
Insbesondere ist  $\chi(n) = 1$ , d.h. es gibt Elemente  $a \in G$  mit  $ord_{\mathbb{F}^*}(a) = n$ .



Beispiel:

- $N = 13$ ,  $\varphi(\varphi(13)) = \varphi(12) = 4$   
primitive Elemente 2, 6, 7, 11
- Ordnungen in  $\mathbb{Z}_{13}^*$

|               |   |    |   |   |   |    |    |   |   |    |    |    |
|---------------|---|----|---|---|---|----|----|---|---|----|----|----|
| $a$           | 1 | 2  | 3 | 4 | 5 | 6  | 7  | 8 | 9 | 10 | 11 | 12 |
| $ord_{13}(a)$ | 1 | 12 | 3 | 6 | 4 | 12 | 12 | 4 | 3 | 6  | 12 | 2  |

- 2 als primitives Element von  $\mathbb{Z}_{13}^*$

|                     |    |    |   |   |   |    |    |    |   |   |    |    |
|---------------------|----|----|---|---|---|----|----|----|---|---|----|----|
| $k$                 | 0  | 1  | 2 | 3 | 4 | 5  | 6  | 7  | 8 | 9 | 10 | 11 |
| $2^k$               | 1  | 2  | 4 | 8 | 3 | 6  | 12 | 11 | 9 | 5 | 10 | 7  |
| $ord_{13}(2^k)$     | 1  | 12 | 6 | 4 | 3 | 12 | 2  | 12 | 3 | 4 | 6  | 12 |
| $\text{ggT}(k, 12)$ | 12 | 1  | 2 | 3 | 4 | 1  | 6  | 1  | 4 | 3 | 2  | 1  |



Beispiel:

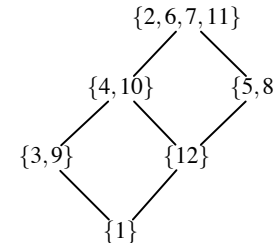
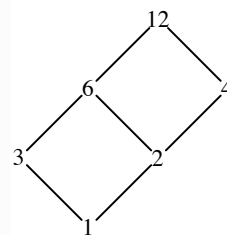
- ▶  $N = 17$ ,  $\varphi(\varphi(17)) = \varphi(16) = 8$   
primitive Elemente 3, 5, 6, 7, 10, 11, 12, 14
- ▶ Ordnungen in  $\mathbb{Z}_{17}^*$

|               |   |   |    |   |    |    |   |   |    |    |    |    |    |    |    |    |
|---------------|---|---|----|---|----|----|---|---|----|----|----|----|----|----|----|----|
| $a$           | 1 | 2 | 3  | 4 | 5  | 6  | 7 | 8 | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| $ord_{17}(a)$ | 1 | 8 | 16 | 4 | 16 | 16 | 8 | 8 | 16 | 16 | 16 | 4  | 16 | 8  | 2  |    |

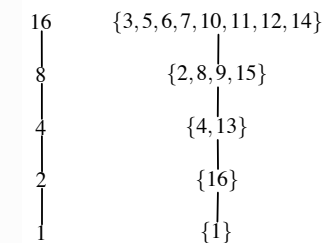
- ▶ 7 als primitives Element von  $\mathbb{Z}_{17}^*$

|                 |   |    |    |    |   |    |   |    |    |    |    |    |    |    |    |    |
|-----------------|---|----|----|----|---|----|---|----|----|----|----|----|----|----|----|----|
| $k$             | 0 | 1  | 2  | 3  | 4 | 5  | 6 | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 |
| $7^k$           | 1 | 7  | 15 | 3  | 4 | 11 | 9 | 12 | 16 | 10 | 2  | 14 | 13 | 6  | 8  | 5  |
| $ord_{17}(7^k)$ | 1 | 16 | 8  | 16 | 4 | 16 | 8 | 16 | 2  | 16 | 8  | 16 | 4  | 16 | 8  | 16 |
| $ggt(k, 16)$    | 1 | 1  | 2  | 1  | 4 | 1  | 2 | 1  | 8  | 1  | 2  | 1  | 4  | 1  | 2  | 1  |

Struktur von  $\mathbb{Z}_{13}^*$



Struktur von  $\mathbb{Z}_{17}^*$



## Endliche Körper

- ▶ Ist  $\mathbb{F}$  ein endlicher Körper, so gibt es eine eindeutig bestimmte Primzahl  $p$  mit  $p \cdot 1 = \underbrace{1 + 1 + \dots + 1}_p = 0$ .  
Dieses  $p$  nennt man die "Charakteristik" von  $\mathbb{F}$ .
- ▶ Ist  $\mathbb{F}$  ein endlicher Körper der Charakteristik  $p$ , so hat  $\mathbb{F}$   $p^n$  Elemente für ein  $n \geq 1$ .
- ▶ Zu jeder Primzahl  $p$  und jedem  $n \geq 1$  existiert ein Körper mit  $p^n$  Elementen.
- ▶ Alle Körper mit  $p^n$  Elementen sind "isomorph".
- ▶ Speziell für  $n = 1$ : diese Körper sind die  $\mathbb{Z}_p$ .
- ▶ Körper mit  $p^n$  Elementen ( $n > 1$ ) entstehen aus  $\mathbb{Z}_p$  durch "algebraische Erweiterung".  
(Sie haben nichts mit  $\mathbb{Z}_{p^n}$  zu tun!)

## Primzahlkriterium

- ▶ Für  $n \in \mathbb{N}$  gilt:

$$n \text{ ist Primzahl} \Leftrightarrow \exists a \in \mathbb{Z}_n^* : ord_n(a) = n - 1$$

- ▶ Beweis:

- ▶  $\Rightarrow$ :  $n$  Primzahl  $\rightarrow \mathbb{Z}_n$  Körper  $\rightarrow \mathbb{Z}_n^*$  zyklisch mit  $\#\mathbb{Z}_n^* = n - 1$ .
- ▶  $\Leftarrow$ : Aus  $\#\mathbb{Z}_n^* = n - 1 = \varphi(n)$  folgt bereits, dass  $n$  Primzahl.

- ▶ Wichtige Bemerkung: das ist ein *existentielles* Kriterium für Primheit! Ein solches  $a$  ist Zeuge dafür, dass  $n$  Primzahl ist.

- Das Ordnungskriterium:

$$ord_n(a) = n - 1 \Leftrightarrow \begin{cases} a^{n-1} \equiv 1 \pmod{n} \\ \forall_{1 \leq t < n-1} a^t \not\equiv 1 \pmod{n} \end{cases} \wedge$$

- Das Ordnungskriterium präzisiert:

$$ord_n(a) = n - 1 \Leftrightarrow \begin{cases} a^{n-1} \equiv 1 \pmod{n} \\ \forall_{\substack{1 \leq t < n-1 \\ t | (n-1)}} a^t \not\equiv 1 \pmod{n} \end{cases} \wedge$$

- Das Ordnungskriterium ganz ökonomisch:

$$ord_n(a) = n - 1 \Leftrightarrow \begin{cases} a^{n-1} \equiv 1 \pmod{n} \\ \forall_{p \text{ prim}, p | n-1} a^{(n-1)/p} \not\equiv 1 \pmod{n} \end{cases} \wedge$$



- Das ganz ökonomische Primzahlkriterium (E. LUCAS):

$$n \text{ ist Primzahl} \Leftrightarrow \exists a \in \mathbb{Z}_n^* : \begin{cases} a^{n-1} \equiv 1 \pmod{n} \\ \forall_{p \text{ prim}, p | n-1} a^{(n-1)/p} \not\equiv 1 \pmod{n} \end{cases}$$

- Also: Primheit von  $n$  lässt sich mittels  $k + 1$  Exponentiationen modulo  $n$  verifizieren, wobei  $k =$  Anzahl der Primteiler von  $n$ .
- Die Ökonomie hat ihren Preis: das Kriterium ist rekursiv!
- Ist das noch effizient verifizierbar?
- JA!  
 V. PRATT: *Every prime has a succinct certificate*,  
 SIAM Journal on Computing, 4 (1975), 214-220.



## Zertifikate für Primzahlen

Zertifikat  $C(n)$  für die Primheit von einer Primzahl  $n$ :

- Angabe einer Faktorisierung

$$n - 1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

wobei die  $p_i$  ganze Zahlen  $\geq 2$  und die  $\alpha_i$  ganze Zahlen  $\geq 1$  sind;

- Nachweis, dass die Zahlen  $p_1, \dots, p_k$  Primzahlen sind, durch Angabe von Zertifikaten  $C(p_i)$  für die  $p_i > 2$ ;
- Angabe einer positiven Zahl  $a < n$  mit

$$a^{n-1} \equiv 1 \pmod{n} \text{ und } a^{(n-1)/p_i} \not\equiv 1 \pmod{n} \quad (1 \leq i \leq k).$$



- 79 ist Primzahl, denn es gilt
  - $79 - 1 = 78 = 2 \cdot 3 \cdot 13$
  - 2, 3 und 13 sind Primzahlen
  - $3^{78} \equiv 1, 3^{78/2} \equiv 78, 3^{78/3} \equiv 23, 3^{78/13} \equiv 18 \pmod{79}$

d.h.  $C(79) = [ 2 \cdot 3 \cdot 13 ; C(3), C(13) ; 3 ]$  ist ein Prim-Zertifikat für 79.

- 13 ist eine Primzahl, denn es gilt
  - $13 - 1 = 12 = 2^2 \cdot 3$
  - 2 und 3 sind Primzahlen
  - $2^{12} \equiv 1, 2^6 \equiv 12, 2^4 \equiv 3 \pmod{13}$
 d.h.  $C(13) = [ 2^2 \cdot 3 ; C(3) ; 2 ]$  ist ein Prim-Zertifikat für 13.
- 3 ist Primzahl, denn es gilt
  - $3 - 1 = 2 = 2$
  - 2 ist Primzahl
  - $2^2 \equiv 1, 2^1 \equiv 2 \pmod{3}$
 d.h.  $C(3) = [ 2 ; - ; 2 ]$  ist ein Prim-Zertifikat für 3.



Ein grösseres Beispiel:

►  $N = 1653701519$  ist Primzahl, denn:

$$N - 1 = 2 \cdot 7 \cdot 19 \cdot 23 \cdot 137 \cdot 1973, \quad 7^{N-1} \equiv 1 \pmod{N} \text{ und}$$

- ◇ 2 ist Primzahl und  $7^{(N-1)/2} \equiv 1653701518 \pmod{N}$
- ◇ 7 ist Primzahl und  $7^{(N-1)/7} \equiv 356579618 \pmod{N}$
- ◇ 19 ist Primzahl und  $7^{(N-1)/19} \equiv 120777631 \pmod{N}$
- ◇ 23 ist Primzahl und  $7^{(N-1)/23} \equiv 1080868740 \pmod{N}$
- ◇ 137 ist Primzahl und  $7^{(N-1)/137} \equiv 101758286 \pmod{N}$
- ◇ 1973 ist Primzahl und  $7^{(N-1)/1973} \equiv 1287679432 \pmod{N}$



► 1973 ist Primzahl, denn:

$$1972 = 2 \cdot 2 \cdot 17 \cdot 29, \quad 3^{1972} \equiv 1 \pmod{1973} \text{ und}$$

- ◇ 2 ist Primzahl und  $3^{1972/2} \equiv 1972 \pmod{1973}$
- ◇ 17 ist Primzahl und  $3^{1972/17} \equiv 273 \pmod{1973}$
- ◇ 29 ist Primzahl und  $3^{1972/29} \equiv 934 \pmod{1973}$

► 137 ist Primzahl, denn:

$$136 = 2 \cdot 2 \cdot 2 \cdot 17, \quad 3^{136} \equiv 1 \pmod{137} \text{ und}$$

- ◇ 2 ist Primzahl und  $3^{136/2} \equiv 136 \pmod{137}$
- ◇ 17 ist Primzahl und  $3^{136/17} \equiv 122 \pmod{137}$



► 29 ist Primzahl, denn:

$$28 = 2 \cdot 2 \cdot 7, \quad 2^{28} \equiv 1 \pmod{29} \text{ und}$$

- ◇ 2 ist Primzahl und  $2^{28/2} \equiv 28 \pmod{29}$
- ◇ 7 ist Primzahl und  $2^{28/7} \equiv 16 \pmod{29}$

► 23 ist Primzahl, denn:

$$22 = 2 \cdot 11, \quad 5^{22} \equiv 1 \pmod{23} \text{ und}$$

- ◇ 2 ist Primzahl und  $5^{22/2} \equiv 22 \pmod{23}$
- ◇ 11 ist Primzahl und  $5^{22/11} \equiv 2 \pmod{23}$

► 19 ist Primzahl, denn:

$$18 = 2 \cdot 3 \cdot 3, \quad 2^{18} \equiv 1 \pmod{19} \text{ und}$$

- ◇ 2 ist Primzahl und  $2^{18/2} \equiv 18 \pmod{19}$
- ◇ 3 ist Primzahl und  $2^{18/3} \equiv 7 \pmod{19}$



► 17 ist Primzahl, denn:

$$16 = 2 \cdot 2 \cdot 2 \cdot 2, \quad 3^{16} \equiv 1 \pmod{17} \text{ und}$$

- ◇ 2 ist Primzahl und  $3^{16/2} \equiv 16 \pmod{17}$

► 11 ist Primzahl, denn:

$$10 = 2 \cdot 5, \quad 2^{10} \equiv 1 \pmod{11} \text{ und}$$

- ◇ 2 ist Primzahl und  $2^{10/2} \equiv 10 \pmod{11}$
- ◇ 5 ist Primzahl und  $2^{10/5} \equiv 4 \pmod{11}$



► 7 ist Primzahl, denn:

$$6 = 2 \cdot 3, \quad 3^6 \equiv 1 \pmod{7} \text{ und}$$

$$\diamond 2 \text{ ist Primzahl und } 3^{6/2} \equiv 6 \pmod{7}$$

$$\diamond 3 \text{ ist Primzahl und } 3^{6/3} \equiv 3 \pmod{7}$$

► 5 ist Primzahl, denn:

$$4 = 2 \cdot 2, \quad 2^4 \equiv 1 \pmod{5} \text{ und}$$

$$\diamond 2 \text{ ist Primzahl und } 2^{4/2} \equiv 4 \pmod{5}$$

► 3 ist Primzahl, denn:

$$2 = 2, \quad 2^2 \equiv 1 \pmod{3} \text{ und}$$

$$\diamond 2 \text{ ist Primzahl und } 2^{2/2} \equiv 2 \pmod{3}$$

Als "Zertifikate" geschrieben:

$$C(1653701519) = [2 \cdot 7 \cdot 19 \cdot 23 \cdot 137 \cdot 1973; C(7), C(19), C(23), C(137), C(1973); 7]$$

$$C(1973) = [2^2 \cdot 17 \cdot 29; C(17), C(29); 3]$$

$$C(137) = [2^3 \cdot 17; C(17); 3]$$

$$C(29) = [2^2 \cdot 7; C(7); 2]$$

$$C(23) = [2 \cdot 11; C(11); 5]$$

$$C(19) = [2 \cdot 3^2; C(3); 2]$$

$$C(17) = [2^4; -; 3]$$

$$C(11) = [2 \cdot 5; C(5); 2]$$

$$C(7) = [2 \cdot 3; C(3); 3]$$

$$C(5) = [2^2; -; 2]$$

$$C(3) = [2; -; 2]$$

## Aufwand der Prim-Verifikation

Aufwandsabschätzung für das Überprüfen eines Zertifikats  $C(n)$ :

$T(n)$  = Anzahl der Verifikationen von Produkten

$$m \stackrel{?}{=} q_1^{\beta_1} q_2^{\beta_2} \cdot \dots$$

und von mod- $q$ -Berechnungen

$$x \stackrel{?}{\equiv} 1 \pmod{q}$$

die für das Überprüfen von  $C(n)$  benötigt werden.

► Rekursion: Für  $n - 1 = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$

$$T(n) = 1 + \sum_{i=2}^k T(p_i) + k + 1$$

Dabei ist  $p_1 = 2$ , und  $C(2)$  ist "kostenlos", d.h.  $T(2) = 0$ .

► Setze  $S(n) = T(n) + 1$ , dann ist

$$S(n) = \sum_{i=2}^r S(p_i) + 4$$

- ▶ Verifiziere per Induktion, dass für alle Primzahlen  $n$ :

$$S(n) \leq 4 \cdot \log_2 n$$

- ▶ Für  $n = 2$  ist nichts zu zeigen.
- ▶ Für Primzahlen  $n > 2$  mit

$$n - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \quad (p_1 = 2)$$

gilt dann:

$$\begin{aligned} S(n) &\leq \sum_{i=2}^k (4 \cdot \log_2 p_i) + 4 = 4 \cdot \sum_{i=1}^k \log_2 p_i \\ &= 4 \cdot \log \prod_{i=1}^k p_i \leq 4 \cdot \log n \end{aligned}$$

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

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

Der AKS-Algorithmus

- ▶ ist verblüffend einfach ( $\Rightarrow$  folgende Seite)
- ▶ die Begründung der Korrektheit ist nicht ganz so einfach, aber interessierten Studenten durchaus zugänglich
- ▶ hat eine (bewiesene!) Laufzeit  $\mathcal{O}(\log^{12} n)$  (aber vermutlich real noch deutlich besser)
- ▶ Hinweis: sehr instruktiver Artikel mit vielen weiteren Hinweisen  
 F. BORNEMANN, PRIMES is in P: Ein Durchbruch für "Jedermann", *Mitteilungen der Deutschen Mathematiker-Vereinigung*, 4-2002, 14–21.  
 engl. Übersetzung: PRIMES is in P: A Breakthrough for "Everyman", *Notices of the American Mathematical Society* 50/5 (2003), 545–552.

- ▶ Beachte: alle Operationen (inklusive Exponentiationen (!!)) mod  $q$ ) werden mit Zahlen mit  $\leq \log n$  Binärstellen durchgeführt — insgesamt ist der Rechenaufwand für das Verifizieren von  $C(n)$  polynomial in  $\log n$ .
- ▶ Ganz wichtig: der Aufwand für das Finden der Zertifikate wird nicht berücksichtigt – es geht ausschliesslich um das Verifizieren!
- ▶ Fazit: Primheit lässt sich effizient *verifizieren*,

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

- ▶ Tatsächlich gilt sogar: Primheit lässt sich effizient *entscheiden*

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

Aber das weiss man erst seit 2002.

Der Algorithmus von AGRAWAL, KAYAL, SAXENA

```

Input: integer  $n > 1$ 
if  $n = a^b$  for  $a \in \mathbb{N}$  and  $b > 1$  then
    output COMPOSITE
end if
Find the smallest  $r$  such that  $\text{ord}_r(n) > 4 \log^2 n$ 
if  $1 < (a, n) < n$  for some  $a \leq r$  then
    output COMPOSITE
end if
if  $n \leq r$  then
    output PRIME
end if
for  $a = 1$  to  $\lfloor 2\sqrt{\phi(r)} \log n \rfloor$  do
    if  $(X + a)^n \not\equiv X^n + a \pmod{X^r - 1, n}$  then
        output COMPOSITE
    end if
end for
output PRIME
    
```