

## 6 Primzahltests

Ein Primzahltest ist ein Algorithmus  $\text{Prim}(m)$ , der zu  $m \in \mathbb{N}_+$  entscheidet, ob  $m \in \mathbb{P} \vee m \notin \mathbb{P}$ .

Einteilung der Tests ( $\neg$ -disjunkt):

- a) + Allgemeiner Test ( $\forall m \in \mathbb{N}$ )
  - Spezieller Test (nur gewisse  $m \in \mathbb{N}$ )
- b) + Voll bewiesener Test
  - Test abhängig von einer Vermutung (zB Riemann-Vermutung)
- c) + Sicherer Test
  - Propabilistischer Test (Monte-Carlo-Methode)
- d) + Praktikabler Test (geht für „große“  $m$ )
  - Unpraktischer Test

### Beispiel

- a) Pepins Test: nur für  $F_n = 2^{2^n} + 1$
- d) Naiver Test: Probiere  $a \mid m, \forall a \in \mathbb{N}, 1 < a \leq \sqrt{m}$
- d) Wilsons Test:  $m \in \mathbb{P} \Leftrightarrow (m-1)! \equiv -1 \pmod{m}$ , es sind mindestens  $m$  „Aktionen“ nötig

### Beweis (Wilsons Test)

„ $\Rightarrow$ “:  $m = p \in \mathbb{P}$ . In  $\mathbb{F}_p$ :

$(m-1)! = \prod_{\alpha \in \mathbb{F}_p^\times} \alpha = \bar{1} \cdot (\overline{-1})$ . Paare  $\alpha\alpha^{-1}$  heben sich weg. Wenn  $\alpha \neq \alpha^{-1}$  verbleibt  $\alpha^2 = 1$ , da  $\alpha = \pm 1 \Rightarrow (m-1)! \equiv -1 \pmod{m}$

„ $\Leftarrow$ “:  $m \notin \mathbb{P} \Rightarrow \text{ggT}((m-1)!, m) = d > 1 \Rightarrow (m-1)! \not\equiv -1 \pmod{m}$  (sonst  $d \mid -1$ ) ■

Prinzip moderner PZTests:

Meist ohne Einschränkung  $m > 2, 2 \nmid m$ . (Rechnung für große  $m$  aufwändig, daher gewöhnlich erst  $p \mid m$  probiert für die  $p \in \mathbb{P}$ , etwa  $p \leq 100000 \vee p \leq 1000000$ ). Man konstruiert Gruppe  $G_m$  derart, dass die Struktur von  $G_m$  für  $m \in \mathbb{P} \wedge m \notin \mathbb{P}$  verschieden ausfällt. Die Strukturverschiedenheit soll mit möglichst wenig und schnellen Rechnungen festgestellt werden.

EZT: Meist  $G_m = (\mathbb{Z}/m\mathbb{Z})^\times$

Höhere ZT: Etwa  $G_m = (\sigma_k / \sigma_k \cdot m)^\times$ , wobei  $\sigma_k$  ein Ring „ganzer algebraischer Zahlen“, im algebraischen Zahlkörper  $K$  ist.

### Beispiel

$K = \mathbb{Q} + \mathbb{Q}i, \sigma_k = \mathbb{Z} + \mathbb{Z}i$  (Ring der ganzen Gaußschen Zahlen)

Algebraische Geometrie:  $G_r$  konstruiert aus „elliptischer Krume“, die über  $\mathbb{Z}$  definiert ist. Vorzug:

Es gibt  $\infty$  viele elliptische Kurven und Zahlkörper. Man kann versuchen, möglichst „geeignete“ zu finden. Hier  $G_m = (\mathbb{Z}/m\mathbb{Z})^\times$ .

- (A) Ein  $\neg$ -ganz geklückter Versuch  
 Strukturaussage für  $G_p$  ( $p \in \mathbb{P}$ ):  
 Satz von Euler-Fermat:  $\bar{a}^{p-1} = 1$ .

### Definition

Sei ohne Einschränkung  $m > 2, 2 \nmid m$ .  $a \in \mathbb{Z}$  heiße Carmichael-Zeuge (für die Zerlegbarkeit von  $m$ ), wenn gilt:

- (i)  $\text{ggT}(a, m) = 1$
- (ii)  $a^{m-1} \not\equiv 1 \pmod{m}$

Klar: Wenn Zeuge gefunden:  $m \notin \mathbb{P}$ .

Leider:  $\exists m \in \mathbb{N}$  mit  $m \notin \mathbb{P}$ , aber kein Zeuge vorhanden!

### Definition

Solche  $m \notin \mathbb{P}$  (also die mit  $\forall a \in \mathbb{Z}, 1 < a < m, \text{ggT}(a, m) = 1$  ist  $a^{m-1} \equiv 1 \pmod{m}$ ) heißen Carmichael Zahlen.

### Satz 6.1 (Carmichael, $\sim 1920$ )

Sei  $m \in \mathbb{N}_+, m > 2, \mathbb{P}_m := \{p \in \mathbb{P} \mid p \mid m\}$ . Dann:  $m$  ist Carmichael Zahl  $\Leftrightarrow$  Es gelten:

- (i)  $2 \nmid m$
- (ii)  $m$  ist qf (???) ( $\forall p \in \mathbb{P} : v_p(m) \leq 1$ )
- (iii)  $\forall p \in \mathbb{P}_m : p-1 \mid m-1$
- (iv)  $m$  hat mindestens 3 verschiedene Primteiler ( $\#\mathbb{P}_m \geq 3$ )

### Beispiel

Kleinste Carmichael-Zahl:  $m = 561 = 3 \cdot 11 \cdot 17$  - 2, 10, 16  $\mid$  560

### Beweis

„ $\Leftarrow$ “:  $\left. \begin{array}{l} \text{Zeige (i) - (iv)} \\ \text{ggT}(a, m) = 1 \end{array} \right\} \Rightarrow a^{m-1} \equiv 1 \pmod{m}$ .

$\forall p \in \mathbb{P}_m : \text{in } \mathbb{F}_p^\times : \text{ord } \bar{a} \mid p-1 \stackrel{(iii)}{\mid} m-1 \Rightarrow \bar{a}^{m-1} = 1 \text{ in } \mathbb{F}_p \Leftrightarrow a^{m-1} \equiv 1 \pmod{p} \Leftrightarrow p \mid a^{m-1} - 1 \stackrel{(ii)qf}{\Rightarrow} m = \prod_{p \in \mathbb{P}_m} p \mid a^{m-1} - 1 \Rightarrow a^{m-1} \equiv 1 \pmod{m}$

„ $\Rightarrow$ “:  $(-1)$  kein Zeuge  $\Rightarrow (-1)^{m-1} \equiv 1 \pmod{m}$ . Falls  $2 \mid m \Rightarrow -1 \equiv 1 \pmod{m} \Rightarrow m = 1, 2$  (Widerspruch!). Also  $2 \nmid m \leadsto (i)$ .

Zu (ii), (iii):

Für  $p \in \mathbb{P}_m$  ist  $t := v_p(m) \geq 1$ .  $\exists \text{PW } a \pmod{p}$  mit  $\text{ggT}(a, m) = 1$  (Sei  $w \text{ PW } \pmod{p}$ , löse das System  $a \equiv w \pmod{p(ChRS)}, a \equiv 1 \pmod{q(q \in \mathbb{P}, q \neq p)} \Rightarrow q \nmid a, p \nmid a \Rightarrow \text{ggT}(a, m) = 1$ )

In  $(\mathbb{Z}/p^t\mathbb{Z})^\times$  ist  $\bar{a}^{m-1} = 1$  (wegen  $a^{m-1} \equiv 1 \pmod{m} \Rightarrow a^{m-1} \equiv 1 \pmod{p^t} \Rightarrow \text{ord } \bar{a} = \phi(p^t) = p^{t-1}(p-1) \mid m-1 \Rightarrow p-1 \mid m-1 \leadsto (iii)$ )

Wäre  $t > 1 \Rightarrow p \mid m - 1$  (Widerspruch zu  $p \nmid m$ ).

Also  $v_p(m) = 1 \leadsto$  (ii)

Noch zu widerlegen:  $\mathbb{P}_m = \{p, q\}, p \neq q$ , etwa  $2 < p < q(\star)$

$m = pq$  laut (ii),  $q - 1 \mid m - 1 = pq - 1 = p(q - 1) + p - 1 \Rightarrow q - 1 \mid q - 1 \Rightarrow q \leq p$   
(Widerspruch  $(\star)$ ) ■

(B) Ein geglückter Versuch

$m \in \mathbb{N}, m > 2, 2 \nmid m$ . Schreibe  $m - 1 = 2^t \cdot u$  mit  $t = v_2(m - 1)$  also  $2 \nmid u, t > 0$ .

### Definition

$a \in \mathbb{N}$  heie Miller-Zeuge (fr die Zerlegbarkeit von  $m$ ), wenn gilt:

- (i)  $\text{ggT}(a, m) = 1$
- (ii)  $a^u \not\equiv 1 \pmod{m}$
- (iii)  $\forall s \in \{0, \dots, t - 1\} : a^{u2^s} \not\equiv -1 \pmod{m}$

### Satz 6.2

Miller-Rabin-PZTest Sei  $m \in \mathbb{N}, m > 2, 2 \nmid m$ . Dann:  $m \notin \mathbb{P} \Leftrightarrow \exists$  Miller-Zeuge  $a$ .  
( $0 < a < m$ )

Zusatz (Rabin): Es gibt dann hchstens  $\frac{3}{4}\phi(m) \leq \frac{3}{4}(m - 1)$   $\neg$ -Zeugen

$\leadsto$  Liefert voll bewiesenen Test:

Test, ob  $\frac{1}{4}(m - 1) + 1$  as Zeugen sind.

Sobald Zeugen gefunden  $\Rightarrow m \notin \mathbb{P}$ .

Kein Zeuge gefunden  $\Rightarrow m \in \mathbb{P}$ .

Aber immer noch unpraktisch (ca  $\frac{1}{4}m$  Aktionen). Es gibt einen sehr praktischen propabilistischen Test:

Teste, ob  $k$  zufllig ausgewhlte Restklassen  $\bar{a}$  ( $1 < a < m$ ) Zeuge sind (falls  $\text{ggT}(a, m) = d > 1$ , so  $m \notin \mathbb{P}$ , sonst  $\text{ggT}(a, m) = 1$ ). Falls Zeuge gefunden  $\Rightarrow m \notin \mathbb{P}$ . Falls kein Zeuge gefunden: Die WK (???), dass man sich mit der Annahme „ $m$  ist prim“ irrt, ist  $< \frac{1}{4^k}$ .

Fr groe  $m$  scheint die WK sogar viel kleiner als  $\frac{1}{4^k}$ . [experiment. Faktoren]

$m <$	Zeuge, falls $m \notin \mathbb{P}$
2047	2
1373653	$2 \vee 3$
3215031753	$2, 3 \vee 5$

### Beweis

„ $\Leftarrow$ “:  $m = p \in \mathbb{P}, \bar{a} \in \mathbb{F}_p^\times$   
 $\text{ord } \bar{a} \mid \phi(p) = p - 1 = 2^t u$   
 $\text{ord } \bar{a} = 2^s \cdot v, 2 \nmid v, s \leq t, v \mid u$

1. Fall:  $s = 0 \Rightarrow \bar{a}^v = 1 \Rightarrow \bar{a}^u = 1 \Rightarrow a^u \equiv 1 \pmod{p}$ , kein Zeuge

2. Fall:  $s > 0 \Rightarrow \bar{a}^{2^{s-1}v} = 1, \bar{a}^{2^{s-1}v} \equiv -1 \pmod{m}, s \in \{0, \dots, t - 1\} \Rightarrow$  kein Zeuge ■

Weiter bei der letzten Vorlesung:

$$m-1 = 2^t u, 2 \nmid u$$

$$\text{Millerzeuge } a: \text{ggT}(a, m) = 1, a^u \not\equiv 1 \pmod{m}$$

$$\forall s = 0, \dots, t-1 : a^{u2^s} \not\equiv 1 \pmod{m}$$

Rest:

$$m \notin \mathbb{P} \Rightarrow \exists \text{ Millerzeuge}$$

Fall I:  $\#\mathbb{P}_m \geq 2, \mathbb{P}_m = \{p_1, \dots, p_t\}$

$$a \equiv -1 \pmod{p_1}$$

$$a \equiv 1 \pmod{p_j (j > 1)}$$

(mit Chinesischem Restsatz lösen)

$$a^u \equiv (-1)^u \equiv -1 \pmod{p_1}, \text{ also ist } a^u \equiv 1 \pmod{m} \text{ falsch (sonst } -1 \equiv 1 \pmod{p_2} \Rightarrow p_1 = 2 \text{ [Widerspruch!])}, \text{ also } a^u \not\equiv 1 \pmod{m}$$

$$a^{u2^s} \equiv 1^{u2^s} \equiv 1 \pmod{p_j (j > 1)} \Rightarrow a^{u2^s} \equiv -1 \pmod{m} \text{ ist falsch, also } a^{u2^s} \not\equiv 1 \pmod{m}$$

Gesehen:  $a$  ist Millerzeuge

Fall II:  $m = p^t, p \in \mathbb{P}, t > 1$ : ist  $a$  Primitivwurzel  $\pmod{m = p^t}$ , so ist  $a$  Millerzeuge.

$$\text{ord}(\bar{a}) = \phi(p^t) = (p-1)p^{t-1}$$

$$- \Rightarrow \bar{a}^u \neq 1, \text{ weil sonst } \text{ord}(\bar{a}) \mid u \Rightarrow p \mid u \mid m-1 \text{ (Widerspruch zu } p \mid m)$$

$$- \Rightarrow \bar{a}^{u2^s} = -1 \Rightarrow \bar{a}^{u2^{s+1}} = 1 \Rightarrow \text{ord}(\bar{a}) = (p-1)p^{t-1} \mid u2^{s+1} \Rightarrow p \mid u \mid m-1 \text{ (Widerspruch!)} \Rightarrow a^{u2^s} \equiv -1 \pmod{m}$$

Stand der Technik:

- 1.) Primzahlen  $< 10^{130}$  mit guter Sicherheit „leicht“ auffindbar, z.B. mit Miller Rabin
- 2.) Zahlen der Größe  $> 10^{130}$ , erstreckt  $m = pq, p, q \geq 10^{130}$  können nicht faktorisiert werden.

Praktischer Test von Rumely, fast in Polynomial-Zeit, vorhanden (Zeit  $\approx \log(m)^{c \log \log \log m}$ ). Falls die verallgemeinerte Riemann-Vermutung gilt, so ist dieser Test sogar in Polynomial-Zeit.

Kayal, Saxena, Aal 2002: Voll bewiesener Primzahltest in Polynomial-Zeit. Fraglich ob dies ein praktischer Test ist.

Faktorisierung großer Nichtprimzahlen scheint ein viel härteres Problem zu sein.

Idee von Fermat:

$$\mathbb{N}_+ \ni m = x^2 - y^2, x, y \in \mathbb{N}, m = (x-y)(x+y), x \geq y \text{ ist Faktorisierung, wenn } x-y \neq 1, m, x-y=1 \text{ und } x+y \neq m. 1, x+y=m \Rightarrow x = \frac{m+1}{2}, y = \frac{m-1}{2} \text{ also echte Teiler, wenn } x, y \neq \frac{m \pm 1}{2}$$

Viele moderne Tests arbeiten so: Suche  $x, y \in \mathbb{N}$  mit  $x^2 \equiv y^2 \pmod{m}, x \not\equiv \pm y \pmod{m}$

Gute Chance, dass  $\text{ggT}(m, x-y)$  oder  $\text{ggT}(m, x+y)$  echter Teiler von  $m$  ist. Sehr viel Test, um die Suche nach solchen  $x, y$  zu beschleunigen: Siehe z.B. Förster, Algorithmic number theory

## 6.1 Anwendung der EZT in der Kryptographie

Rivests öffentliches Chiffrier System.  $m$  große Zahl.

Nachricht ist hier  $N \in \text{Versys}_m^\times = \{a \in \mathbb{N} \mid 0 < a < m, \geq (a, m) = 1\}$  (Falls  $m = p_1^{n_1} \cdot \dots \cdot p_l^{n_l}, p_1 < \dots < p_l \in \mathbb{P}, n_j \in \mathbb{N}_+$ , so sind alle  $N \in \mathbb{N}$  mit  $1 \leq N < p_1$  im  $\text{Versys}_m$ .  $N$  kodiert Textabschnitt mit  $k$  Zeichen, z.B. Leerstelle = 000, Jedes Zeichen erhält Ziffern  $< 1000$ .

### Beispiel

$N =$

K	O	M	M		N	I	C	H	T	
011	015	013	013	000	014	009	003	008	020	$< 10^{3k}$

### Definition

- (i) Eine Chiffre ist (für uns) eine bijektive Abbildung  $P : \text{Versys}_m^\times \rightarrow \text{Versys}_m^\times, N' = P(N)$  ist die „chiffrierte“ Nachricht.
- (ii) ein „öffentliches Chiffresystem“ ist eine Liste („öffentliches Adressbuch“):  
 $(T, P_T), T \in \tau = \text{Menge von Teilnehmern. } P_T \text{ Chiffre, derart, dass } T \neq T' \Rightarrow P_T \neq P_{T'}$ 
  - (a) Jeder Teilnehmer  $T \in \tau$  erhält das Adressbuch  $(T, P_T)_{T \in \tau}$
  - (b)  $T$  und nur  $T$  erhält  $P_T^{-1}$  (Umkehrabbildung von  $P_T$ )  
 Praktisch:  $T$  muss  $P_T^{-1}$  besonders gut sichern, gegen Diebstahl, Ausspähen, Hacker, usw.

### Technische Anforderungen:

- 1.)  $P_T(N), P_T^{-1}(N)$  müssen in vernünftiger Realzeit berechenbar sein
- 2.) Nicht einmal ein Supercomputer kann  $P_T^{-1}$  aus  $P_T$  ermitteln ( $P_T$  Trapdoor-Funktion)
- 3.) Nur  $T$  hat  $P_T^{-1}$ . Der Systemadministrator hat am Anfang die  $P_T$ 's und die  $P_T^{-1}$ 's. Nach Absenden von  $P_T^{-1}$  an  $T$  vernichtet er  $P_T^{-1}$

### Anwendungen:

- I) Geheime Nachricht über öffentlich zugängliche Kanäle (etwa Internet) übermitteln  $T$  von  $A$  zu  $B, A, B \in \tau$  ohne das Unbefugte  $N$  gewinnen können.

Methode:  $A$  berechnet  $P(N) = N'$  und sendet  $N'$  an  $B$ . Nur  $B$  kann aus  $N'$  wieder  $N = P_B^{-1}(N')$  ermitteln.

Beispiel:

- $A$  Spion des Geheimdienstes,  $B =$  Geheimdienstzentrale,  $C, D$  die gegnerischen Geheimdienste
- $A$  ist Bank,  $B$  ist Kunde,  $N$  = Kontostand

- II) Geheimnachricht mit elektronischer Unterschrift

Methode:  $A$  sendet an  $B$ : „ $N = P_B P_A^{-1}(N)$ , Gruß  $A$ “. Nur  $A$  kann  $N'$  herstellen, nur  $B$  kann daraus  $N = P_A P_B^{-1}(N')$  gewinnen.

Beispiel:

$A = \text{Kunde}$ ,  $B = \text{Bank}$ ,  $N = \text{„Überweisen Sie 200'000.- von meinem Konto an } C\text{“}$

III) Sichere Speicherung von Nachrichten

Methode: Speichere  $N' = P_{A_t}^{-1}(N) \dots P_{A_1}^{-1}(N)$ . Benötigt werden  $A_1, \dots, A_t \in \tau(t=1)$ . Nur mit Willen von allen Mitwirkenden  $A_1, \dots, A_t$  kann  $N$  aus  $N'$  wieder rekonstruiert werden.

EZT kann z.B. zum Erfüllen der technischen Voraussetzungen verwendet werden.

Rivests Vorschlag  $\subseteq$  RSA-Code (Rinest, Shamn, Adleman 1978)

Adressbuch: Liste( $T, m_T, s_T$ ),  $m_T, s_T \in \mathbb{N}$ ,  $m_T = p_1^{n_1} \dots p_l^{n_l}$ ,  $p_i$  zu Anfang dem Administrator bekannt, öffentlich nur  $m_T$ 's,  $s_T$ 's ziemlich groß.

Chiffre  $P_T(N) := (N^{s_T} \bmod m_i)$ . Dann theoretisch  $P_T^{-1}(N') = N^{t_T}$ , wobei  $t_T s_T \equiv 1 \bmod \phi(N)$  (Euler Funktion). Hiermit erhält  $T$  auch noch  $t_T$ .  $t_T$  ist nur berechenbar, wenn  $\phi(m) = m \prod_{p|m} (1 - \frac{1}{p})$  bekannt, dass geht nur (nach heutigem Wissen), wenn Primzerlegung, also die  $p_i$  bekannt sind.