Aufgabe (zum Chinesischen Restsatz)

Seien $m=5$ und $n=9$ zwei teilerfremde Zahlen. Der CR besagt, dass $x \circ\!\!-\!\!\bullet (a,b)$ eine bijektive Abbildung zwischen $\mathbb{Z}_{5\cdot 9}$ und $\mathbb{Z}_5 \times \mathbb{Z}_9$ darstellt, wobei $a = x \bmod 5$ und $b = x \bmod 9$. Wie man die Umkehrung (von a,b nach x) berechnet, wird im Beweis des CR angegeben.

Man stelle eine Tabelle auf als 5×9 Matrix, die diese bijektive Abbildung beschreibt.

Hinweis: Es muss nicht gerechnet werden, die Tabelle kann rein „mechanisch" ausgefüllt werden.

Antwort:

a \ b	0	1	2	3	4	5	6	7	8
0	0	10	20	30	40	5	15	25	35
1	36	1	11	21	31	41	6	16	26
2	27	37	2	12	22	32	42	7	17
3	18	28	38	3	13	23	33	43	8
4	9	19	29	39	4	14	24	34	44

z.B: $33 \circ\!\!-\!\!\bullet (3,6)$

Die Zahlen $0, 1, \ldots, 44$ eintragen mit „wrap-around".

Aufgabe: 9 Piraten erbeuten einen Schatz mit Goldmünzen. (Es sind nicht mehr als 500 Münzen). Da sie nicht zählen bzw. rechnen können, verteilen sie den Schatz Münze für Münze unter sich auf. Es geht aber nicht auf: es bleiben 4 Münzen übrig. Darüber geraten sie so in Streit, bis einer der Piraten dabei ums Leben kommt. Nun teilen sie erneut unter 8 Piraten auf. Diesmal bleiben 3 Münzen übrig. Erneuter Streit endet mit 7 überlebenden Piraten. Beim erneuten Aufteilen geht es genau auf. Jeder der 7 Piraten erhält 1/7 des Goldschatzes.
Wieviele Münzen waren es?

Lösung: Gesucht ist $x \leq 500$ so dass

$$x \equiv 4 \pmod 9$$
$$x \equiv 3 \pmod 8$$
$$x \equiv 0 \pmod 7$$

Da 9, 8, 7 paarweise teilerfremd sind, können wir den C.R. anwenden.

Wir berechnen die verschiedenen notwendigen Hilfszahlen, um x zu berechnen:

$$n = 9 \cdot 8 \cdot 7 = 504$$

$$m_1 = \frac{n}{9} = 8 \cdot 7 = 56$$

$$m_2 = \frac{n}{8} = 9 \cdot 7 = 63$$

$$m_3 = \frac{n}{7} = 8 \cdot 9 = 72$$

Als Nächstes müssen modulo 9, 8 bzw. 7 multiplikative Inverse berechnet werden. Daher notieren wir alle Inversen:

$$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$$

Inverse mod 9

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

Inverse mod 8

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

Inverse mod 7

Nun gilt: $m_1 = 56 \equiv 2 \pmod 9$; invers ist $y_1 = 5$

$m_2 = 63 \equiv 7 \pmod 8$; invers ist $y_2 = 7$

$m_3 = 72 \equiv 2 \pmod 7$; invers ist $y_3 = 4$

Die gesuchte Zahl x ergibt sich laut Beweis des CR als

$$x = \left(\sum_{j=1}^{3} a_j \cdot y_j \cdot m_j \right) \mod n$$

$$= (4 \cdot 5 \cdot 56 + 3 \cdot 7 \cdot 63 + 0 \cdot 4 \cdot 72) \mod 504$$

$$= 2443 \mod 504 = \underline{\underline{427}}$$

Es sind 427 Münzen.

Aufgabe: Sei $n = 113$. Man berechne das Profil von $a = 2$ modulo n.

Antwort: Es ist $n - 1 = 112 = 2^4 \cdot 7$. Das Profil von a besteht also aus 5 Komponenten:

$(2^{112} \mod 113,\ 2^{56} \mod 113,\ 2^{28} \mod 113,\ 2^{14} \mod 113,$

$2^7 \mod 113)$

$= (1, 1, 1, -1, 15)$ ... reguläres Profil.

$n = 113$ ist vermutlich Primzahl. Um ganz sicher zu sein, müsste man noch mehr Basiszahlen als die 2 probieren.

Aufgabe: Berechne das Profil von 2 modulo 561.

Antwort: Für $n = 561$ ist $n-1 = 560 = 2^4 \cdot 35$

Das Profil ist also:

$$(2^{560} \bmod 561,\ 2^{280} \bmod 561,\ 2^{140} \bmod 561,\ 2^{70} \bmod 561,$$
$$2^{35} \bmod 561) =$$

$$(1, 1, \underline{67}, 166, 263) \quad \text{--- irreguläres Profil}$$

561 besteht den „Fermat-Test" zur Basis 2. Da 561 eine „Carmichael-Zahl" ist, besteht sie den Fermat-Test für alle Basen $\in \mathbb{Z}_{561}^*$.

Dies zeigt, dass 561 definitiv keine Primzahl ist.

Es gilt:
$561 = 3 \cdot 11 \cdot 17$

Also ist
$\varphi(561) = 2 \cdot 10 \cdot 16$
$= 320.$

Also ist die Wahrscheinlichkeit, den Fermat-Test zu bestehen: $\frac{\varphi(561)}{560} = \frac{320}{560} = \frac{4}{7} \approx 0{,}57.$

Bei allen Carmichael-Zahlen ist diese W'heit sehr hoch. Erst durch den „Profil-Test" erkennt man mit hoher W'heit, dass keine Primzahl vorliegt.

Der Miller-Rabin-Primzahltest:

Idee: Gegeben: ungerade Zahl n (soll auf Primzahleigenschaft getestet werden).

- Wähle $a \in \mathbb{Z}_n^*$ zufällig.

  (Eigentlich: Wähle $a < n$ zufällig, aber falls $ggT(a,n) > 1$, so ist n sicher keine Primzahl.)

- Teste, ob $\underbrace{a^{n-1} \equiv 1 \pmod n}$ „Fermat-Test"

  also:

  $$\text{modexp}(a, n-1, n) \stackrel{?}{=} 1$$

Jede Primzahl besteht diesen Test ($\hat{=}$ kleiner Satz von Fermat). Viele Nicht-Primzahlen bestehen den Test nicht.

Bem: Der obige Test $ggT(a,n) \stackrel{?}{=} 1$ kann wegfallen, denn falls $ggT(a,n) > 1$, also $a \notin \mathbb{Z}_n^*$, so ist $a^{n-1} \not\equiv 1 \pmod n$. Man kann sich also auf den Fermat-Test beschränken.

- Sei nun $n-1 = 2^k \cdot u$ (u ungerade, $k \geq 1$). Nun wird getestet, ob das Profil

$$\left(\underbrace{a^{n-1} \bmod n}_{=1}, a^{\frac{n-1}{2}} \bmod n, \ldots, a^{\overbrace{\frac{n-1}{2^k}}^{=u}} \bmod n\right)$$

regulär ist. Falls dies irregulär ist, so ist n sicher keine Primzahl.

- Das Verfahren ggf. mit mehreren Basen a wiederholen.

Bemerkung: Die Binärdarstellung der Zahl $n-1$ hat folgende Form: $n-1 = (1 \ldots\ldots 0 0 \ldots 0)_2$ mit $\overleftarrow{\quad k \geq 1 \quad}$

Im Zuge der Berechnung von modexp$(a, n-1, n)$ werden die Zahlen im Profil von a (mod n) sowieso berechnet. Daher kann man den Test auf irreguläres Profil in die Berechnung von $a^{n-1} \bmod n$ integrieren:

Eingabe $n > 2$ (ungerade Zahl)

Wähle $a < n$ zufällig.

Die Binärdarstellung von $n-1$ sei

$$(b_{m-1}\, b_{m-2} \cdots b_1\, b_0)_2$$

$$\| \quad 0$$

```
d := 1; d1 := 1;
for i := m-1 to 0 do
    d := (d * d) mod n;
    if b_i = 1 then d := (d * a) mod n;
    if d = 1 and d1 ∉ {1, n-1} then
        „keine Primzahl"
    d1 := d;
if d ≠ 1 then „keine Primzahl"
else „wahrscheinlich Primzahl".
```

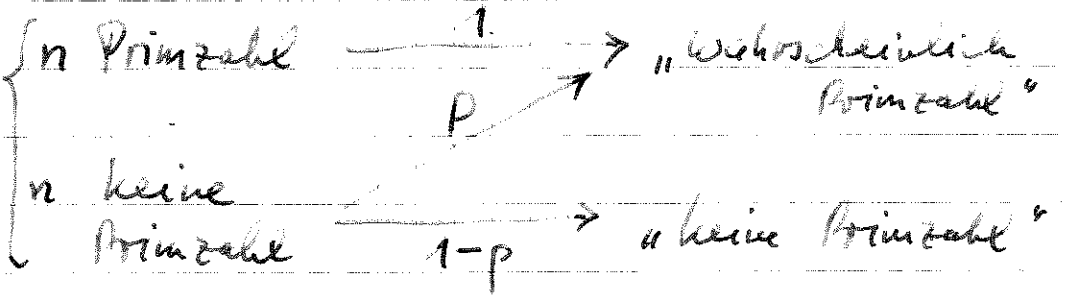
Beispiel: $n = 85 = 5 \cdot 17$ ist keine Primzahl.

Es gilt: $n-1 = 84 = 2^2 \cdot 21$.

Von den $a < 85$ bestehen 16 davon den Fermat-Test $a^{84} \stackrel{?}{\equiv} 1 \pmod{85}$.

Von diesen 16 a's bestehen nur noch 4 den Profit-Test. Die „Fehlerwahrscheinlichkeit" ($\hat{=} P($„wahrscheinlich Primzahl"$)$) beträgt bei $n = 85$ als Eingabe also $\frac{4}{84} \approx 5\%$.

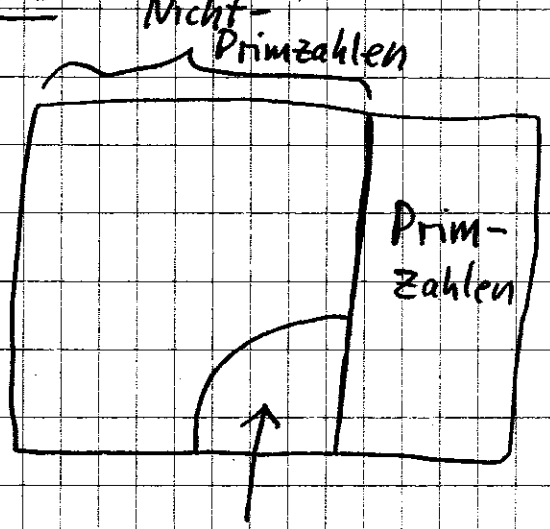
Allgemein:



Wie groß ist p im worst case?

(Wir werden zeigen: $p = \frac{1}{4}$).

Überblick:



Carmichael-Zahlen: dies sind keine Primzahlen, sie bestehen aber den Fermat-Test $a^{n-1} \equiv 1 \pmod n$ für alle $a \in \mathbb{Z}_n^*$.

Die erste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$, die nächste ist $1105 = 5 \cdot 13 \cdot 17$. Carmichael-Zahlen bestehen immer aus ≥ 3 ungeraden Primfaktoren. Das bedeutet: modulo einer Carmichael-Zahl hat die 1 immer $2^3 = 8$ verschiedene Quadratwurzeln, also außer 1 und $n-1$ noch 6 weitere. (Falls $n = p \cdot q \cdot r$, so erhält man die Quadratwurzeln durch $(\pm 1 \bmod p, \pm 1 \bmod q, \pm 1 \bmod r) \longrightarrow x_{1-8}$. Die Rücktransformation nach x erfolgt mit dem C.R.)

Zur Abschätzung der Fehlerwahrscheinlichkeit:

Es gelte $a^{n-1} \equiv 1 \pmod n$, was bei einer Carmichaelzahl für alle $a \in \mathbb{Z}_n^*$, also „fast immer" zutrifft.

Ein etwas informales Argument: Wenn man nun $a^{\frac{n-1}{2}}$ bildet, da a zufällig ist, entsteht auch per Zufall eine der Quadratwurzeln der 1. Sofern n aus ≥ 3 Primfaktoren besteht, so erhält man eine der ≥ 8 Quadratwurzeln. Es entsteht also ein reguläres Profil, was zur falschen Ausgabe „wahrscheinlich Primzahl" führt, mit W'heit

$$\leq \frac{2}{8} = \frac{1}{4}.$$

Nur „normale" Nicht-Primzahlen ist diese W'heit höchstens $2^{-1} = \frac{1}{2}$. Allerdings bestehen diese

„normalen" Nicht-Primzahlen n den Fermat-Test höchstens mit W'heit $\frac{1}{2}$, so dass sich insgesamt ebenfalls eine Fehler w'heit $\leq \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ ergibt. Dies sieht man so:

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

ist eine multiplikative Gruppe. Da dies für „normale" Nicht-Primzahlen eine echte Teilmenge der Gruppe $\mathbb{Z}_n^*$ darstellt, ist $|F_n| \leq \frac{|\mathbb{Z}_n^*|}{2}$. Somit folgt für diese n:

$$P(a \in \mathbb{Z}_n^* \text{ besteht den Fermat-Test}) \leq \frac{1}{2}.$$

---

t-maliges Wiederholen des Miller-Rabin-Primzahltests ~~erf~~ erniedrigt die mögliche Fehlerquote drastisch auf $\left(\frac{1}{4}\right)^t = 2^{-2t}$.

Die Laufzeit von Miller-Rabin ist $O(m^3)$.

Bem: Seit 2002 ist ein deterministischer und polynomieller Algorithmus für das Feststellen der Primzahleigenschaft bekannt („AKS-Algorithmus", nach Agrawal, Kayal, Saxena). Allerdings hat dieser eine Laufzeit von ca. $O(n^{12})$.

Das Eulerkriterium zeigt an, ob $a \in \mathbb{Z}_n^*$ ein Quadratischer Rest modulo n (also eine Quadratzahl) ist, wobei n Primzahl! Dies ist der Fall, genau dann wenn

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

Anders ausgedrückt: Es gilt

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

wobei $\left(\frac{a}{n}\right) = \begin{cases} 1, & \text{falls } a \in QR_n \\ -1, & \text{falls } a \notin QR_n \text{ d.h. } a \in QNR_n \end{cases}$

--- eine Art Indikatorfkt für Quadrate, das Legendre-Symbol.

Aufgabe: $n = 19$ ist Primzahl.

Das Euler-Kriterium zeigt an, dass 5 eine Quadratzahl modulo 19 ist, denn $5^{\frac{19-1}{2}} \equiv 1 \pmod{19}$

Bestimme die 2 Quadratwurzeln der 5!

Lösung: Da $5^9 \equiv 1 \pmod{19}$, ist $5^{10} \equiv 5 \pmod{19}$.

Glücklicherweise ist der Exponent 10 eine gerade Zahl (da die Primzahl n hier die Form hat $n \equiv 3 \pmod 4$), deshalb ist 5^5 eine Quadratwurzel von 5: $5^5 \equiv \underline{\underline{9}} \pmod{19}$.

Die andere Quadratwurzel der 5 ist dann

$-9 \equiv 19 - 9 = \underline{\underline{10}}$.

Probe: $9^2 = 81 \equiv 5 \pmod{19}$

$10^2 = 100 \equiv 5 \pmod{19}$