Zahlentheorie

Quadratische Reste
und
Bekannte Primzahlen

Zahlentheorie

Quadratische Reste – Teil 1

Systeme

Satz 79: $P(x) \equiv 0 \bmod m_1 \cdot m_2 \cdot \ldots \cdot m_r$ ist lösbar für paarweise fremde $m_i \Leftrightarrow$ das System

$$\begin{aligned} P(x) &\equiv 0 \bmod m_1 \\ P(x) &\equiv 0 \bmod m_2 \\ &\vdots \\ P(x) &\equiv 0 \bmod m_r \end{aligned}$$

lösbar ist.

Die Lösungszahl ist dann gleich dem Produkt der Lösungszahlen von $P(x) \equiv 0 \bmod m_i$

Systeme

Beispiel: $x^2 \equiv 1 \mod 3$ besitzt 2 Lösungen $\{1,2\}$

$x^2 \equiv 1 \mod 8$ besitzt 4 Lösungen $\{1,3,5,7\}$

Daher besitzt die Gleichung $x^2 \equiv 1 \mod 24$ 8

Lösungen.

Quadratischer Rest

Definition 80: Sei nun $n \in \mathbb{N}$. Ein Element a heißt quadratischer Rest, wenn es hierzu eine passende Zahl x gibt mit

$$x^2 \equiv a \bmod n$$

andernfalls quadratischer Nichtrest.

Quadratischer Rest

Satz 81: $x^2 \equiv a \bmod n$ mit $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ ist lösbar $\Leftrightarrow$ das System

$$\begin{aligned} x^2 &\equiv a \bmod p_1^{e_1} \\ x^2 &\equiv a \bmod p_2^{e_2} \\ &\vdots \\ x^2 &\equiv a \bmod p_r^{e_r} \end{aligned}$$

lösbar ist.

Quadratischer Rest

Bemerkung:

1. $x^2 \equiv a \mod n$ mit $n = pq \Leftrightarrow$
   $x^2 \equiv a \mod p \wedge x^2 \equiv a \mod q$

2. $0, 1^2, 2^2, \ldots$ sind quadratische Reste zu jedem Modulo n

3. Jede Zahl ist quadratischer Rest modulo 1

Übung

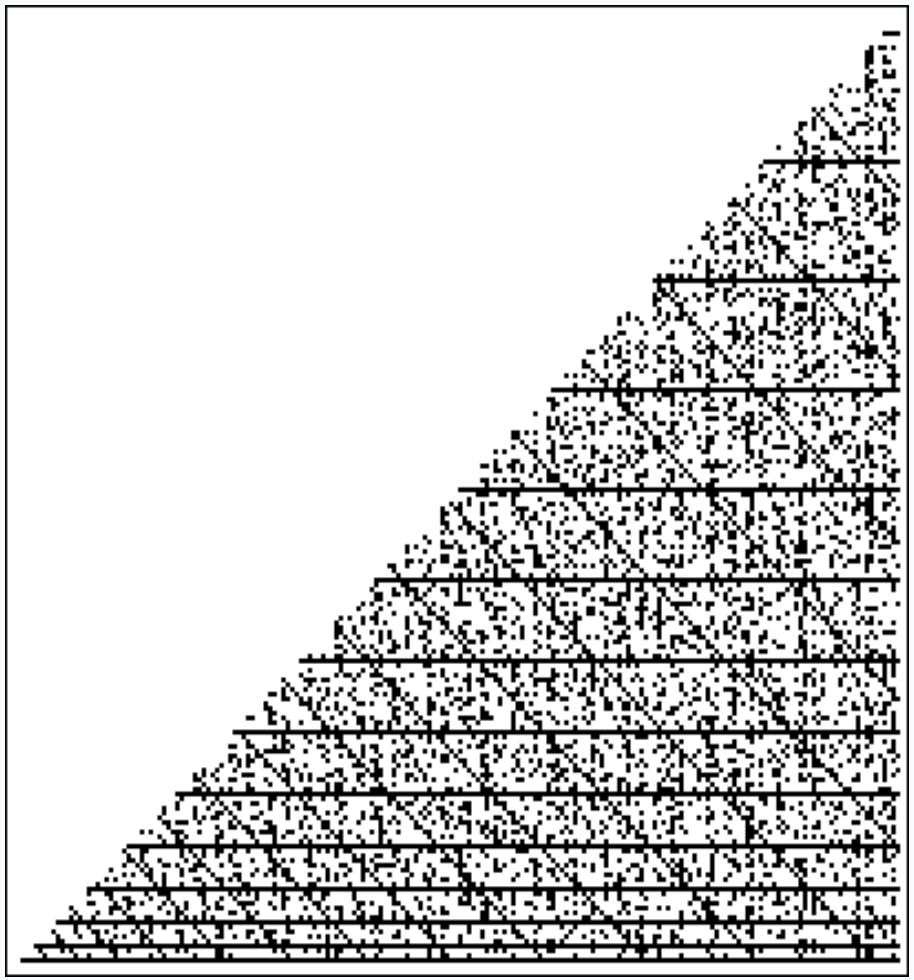
Bemerkung:

4. Ist 3 quadratischer Rest modulo 4? Gesucht:
   $x^2 \equiv 3 \mod 4$ Es ist für:

$$
\begin{aligned}
x = 0: &\quad x^2 = 0 \\
x = 1: &\quad x^2 = 1 \\
x = 2: &\quad x^2 = 4 \equiv 0 \mod 4 \\
x = 3: &\quad x^2 = 9 \equiv 1 \mod 4
\end{aligned}
$$

Also: 3 ist quadratischer Nichtrest (sowie 2, 1 und 0 sind quadratische Reste)

$$x^2 \equiv a \mod n$$



Urbilder

Von oben wissen wir, dass für $n = 8$

$a \in \{0, 1, 4\}$ bzw. $\bar{a} \in \{2, 3, 5, 6, 7\}$

Zum quadratischen Rest existieren dann die Urbilder (Quadratwurzeln). So sind die Quadratwurzeln von $4 \bmod 8$ die Zahlen 2 und 6.

Urbilder

Bemerkung:

Haben wir eine Quadratwurzel x gefunden, also eine Zahl mit

$$x^2 \equiv a \bmod n$$

so ist auch

$$(n - x)^2 = n^2 - 2\mathrm{nx} - x^2 \equiv x^2 \equiv a \bmod n$$

$$\Rightarrow \ (n-x)^2 \equiv a \bmod n$$

Urbilder

Die Quadratwurzeln von $4 \bmod 8$ und $a \bmod 8$:

	x^2-4	
$1 \Rightarrow$	$1-4=-3$	✗
$\mathbf{2 \Rightarrow}$	$\mathbf{4-4=0}$	✓
$3 \Rightarrow$	$9-4=5$	✗
$4 \Rightarrow$	$16-4=12$	✗
$5 \Rightarrow$	$25-4=21$	✗
$\mathbf{6 \Rightarrow}$	$\mathbf{36-4=32}$	✓
$7 \Rightarrow$	$49-4=45$	✗
$8 \Rightarrow$	$64-4=60$	✗

	x^2-a	
$0 \Rightarrow$	$0-0$	♣
$\mathbf{1 \Rightarrow}$	$\mathbf{1-1}$	♥
$2 \Rightarrow$	$4-4$	◆
$\mathbf{3 \Rightarrow}$	$\mathbf{9-1}$	♥
$4 \Rightarrow$	$16-0$	♣
$\mathbf{5 \Rightarrow}$	$\mathbf{25-1}$	♥
$6 \Rightarrow$	$36-4$	◆
$\mathbf{7 \Rightarrow}$	$\mathbf{49-1}$	♥
$8 \Rightarrow$	$64-0$	♣

Übung

Zur weiteren Veranschaulichung betrachte die Fälle $n = 6$ und $n = 7$ dh. suche a für

$x^2 \equiv a \bmod 6$ bzw. $x^2 \equiv a \bmod 7$

x		a		
0	–	0		◆
1	–	1		♣
2	**–**	**4**		♥
3	–	3		♠
4	**–**	**4**		♥
5	–	1		♣
6	–	0		◆

x		a		
0	–	0		◆
1	–	1		♣
2	**–**	**4**		♥
3	–	2		♠
4	–	2		♠
5	**–**	**4**		♥
6	–	1		♣
7	–	0		◆

Legendre Symbol

Definition 82: Legendre Symbol für eine Primzahl $p > 2$ und $p \nmid k$, so ist

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & \text{falls k quadratischer Rest modulo p} \\ -1 & \text{falls k quadratischer Nichtrest modulo p} \end{cases}$$

Es gilt: $\left(\frac{1}{p}\right) = 1$, $\left(\frac{l^2}{p}\right) = 1$

$\left(\frac{3}{7}\right) = -1$ (s.o. 3 taucht als quadr. Rest nicht auf)

Legendre Symbol

Satz 83: Für $p>2$, $p \nmid k_1$ und $k_1 \equiv k_2 \bmod p$ ist

$$\left(\frac{k_1}{p}\right) = \left(\frac{k_2}{p}\right)$$

Beweis: trivial, wg. $x^2 \equiv k_1 \bmod p$ und $k_1 \equiv k_2 \bmod p$ ist auch $x^2 \equiv k_2 \bmod p$ und umgekehrt ($p \nmid k_2$ ergibt sich aus $p \nmid k_1$ und $k_1 \equiv k_2 \bmod p$)

❑

Legendre Symbol

Satz 84: Jedes prime Restsystem besteht aus $\frac{p-1}{2}$ quadratischen Resten und $\frac{p-1}{2}$ quadratischen Nichtresten.

Legendre Symbol

<u>Beweis:</u> Bei modulo p können nur die Zahlen $a \in \{1^2, 2^2, \ldots, (p-1)^2\}$ quadratische Reste sein.

Weil $(p-x)^2 \equiv x^2 \equiv a \bmod p$ ist jeder quadratische Rest von x auch von $p-x$ quadratischer Rest. Wir betrachten daher nur $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$.

Legendre Symbol

Diese Zahlen sind modulo p inkongruent, denn

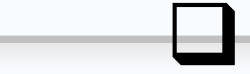
wären zwei Zahlen kongruent, also

$x^2 = y^2 \bmod p$ so wäre (Œ sei $x \geq y$):

$$x^2 - y^2 = (x - y)\cdot(x + y) = kp$$

und wegen $1 \leq x, y \leq \frac{p-1}{2}$ wäre $x + y < p$

und $0 \leq x - y < p$. Damit muss $x = y$ gelten.



Legendre Symbol

Beispiel: $p = 11$

Im primären Restsystem $\{1,2,3,4,5,6,7,8,9,10\}$

sind die Zahlen $\{1,3,4,5,9\}$ quadr. Reste,

$\{2,6,7,8,10\}$ sind die quadr. Nichtreste.

Legendre Symbol

Satz 85:

$$\sum_{k=1}^{p-1} \left(\frac{k}{p} \right) = 0$$

Zur praktischen Berechnung hilft folgender Satz

Satz 86:

$$\left(\frac{k}{p} \right) = k^{\frac{p-1}{2}} \mod p$$

(nach Euler)

Legendre Symbol

<u>Beweis:</u> Nach Fermat gilt $k^{p-1} \equiv 1 \bmod p$

also $p \mid k^{p-1} - 1 = \left(k^{\frac{p-1}{2}} - 1\right) \cdot \left(k^{\frac{p-1}{2}} + 1\right)$.

Sei $\left(\frac{k}{p}\right) = 1$. Dann existiert ein x mit

$$x^2 \equiv k \bmod p$$

und damit $k^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p$

(da $p \nmid k$ gilt auch $p \nmid x$).

Legendre Symbol

Da nun aber mit dieser Lösung bereits $\frac{p-1}{2}$

Lösungen gefunden werden, verbleiben für den

Rest nur die Werte $k^{\frac{p-1}{2}} \equiv -1 \bmod p$

❑

Legendre Symbol

Satz 87: Es gilt

$$\left(\frac{k_1 k_2}{p}\right) = \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right)$$

Also: Das Produkt ist genau dann ein quadratischer Rest, wenn beide Faktoren quadratischer Rest oder quadratischer Nichtrest sind.

Legendre Symbol

Beweis:

$$\left(\frac{k_1 k_2}{p}\right) \underset{\text{Satz 86}}{\equiv} (k_1 \cdot k_2)^{\frac{p-1}{2}} \bmod p$$

$$\equiv k_1^{\frac{p-1}{2}} \cdot k_2^{\frac{p-1}{2}} \bmod p$$

$$\underset{\text{Satz 86}}{\equiv} \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right) \bmod p$$

Die rechte Seite ist -1 oder 1, die linke auch. Daher unterscheiden sich beide Seiten um -2, 0 oder 2.

Legendre Symbol

Da aber $p>2$ und die Werte modulo p kongruent sind (p die Differenz teilen muss), bleibt nur 0 und damit $\left(\frac{k_1 k_2}{p}\right) = \left(\frac{k_1}{p}\right).\left(\frac{k_2}{p}\right)$.

❑

Zahlentheorie

Quadratische Reste und Bekannte Primzahlen

Michael Meiners, Dennis Hahn

Legendre Symbol

Satz: Es gilt

$$\left(\frac{k_1 \cdot k_2 \cdot \ldots \cdot k_r}{p}\right) = \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right) \cdot \ldots\ldots \cdot \left(\frac{k_r}{p}\right)$$

Insbesondere

$$\left(\frac{k_1 \cdot k_2^2}{p}\right) = \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2^2}{p}\right) = \left(\frac{k_1}{p}\right)$$

Legendre Symbol

Daraus ergibt sich, dass man die Bestimmung des Legendre-Symbols zurückführen kann, indem man zunächst alle quadratfreien Anteile herausnimmt und schließlich nur noch die Legendre Symbole für

$$\left(\frac{\pm 1}{p}\right), \left(\frac{2}{p}\right) \text{ und } \left(\frac{q}{p}\right) \text{ für Primzahlen } q \text{ benötigt.}$$

Legendre Symbol

Satz:

1. $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\text{Analog: } 1 \text{ falls } p \equiv 1 \bmod 4$$

2. $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

$$\text{Analog: } 1 \text{ falls } p \equiv \pm 1 \bmod 8$$

Legendre Symbol

3. $\left(\frac{3}{p}\right) = (-1)^{\frac{p+1}{6}}$

$\text{Analog}: 1 \text{ falls } p \equiv \pm 1 \bmod 12$

4. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot a$ (Quadratisches Reziprozitätsgesetz)

mit $a = 1 \text{ falls } p \equiv q \equiv 3 \bmod 4 \text{ sonst } a = -1$

Legendre Symbol

Aufgabe:

Ist 360 quadratischer Rest modulo 127?

$$\left(\frac{k}{p}\right) = \left(\frac{360}{127}\right) = \ldots$$

Legendre Symbol

Lösung

$$\left(\frac{360}{127}\right)=\left(\frac{4\cdot 9\cdot 2\cdot 5}{127}\right)=\left(\frac{2^2}{127}\right)\cdot\left(\frac{3^2}{127}\right)\cdot\left(\frac{2\cdot 5}{127}\right)=\left(\frac{2}{127}\right)\cdot\left(\frac{5}{127}\right)$$

$$\left(\frac{2}{127}\right) = (-1)^{\left(\frac{127^2-1}{8}\right)} = (-1)^{2016} = 1 \Rightarrow \text{aus } 2.$$

$$\left(\frac{5}{127}\right) = -\left(\frac{127}{5}\right) = (-1)\left(\frac{2}{5}\right) = -(-1)^3 = 1 \Rightarrow \text{aus } 4.$$

Legendre Symbol

Satz: Es gibt unendlich viele Primzahlen der Form $p \equiv 1 \bmod 4$

Es ist $\left(\frac{-1}{p}\right) = 1$ falls $p \equiv 1 \bmod 4$

Damit ist für n>1: $x^2 \equiv -1 \bmod p$ Lösbar, falls

$$p \equiv 1 \bmod 4$$

Legendre Symbol

Nun ist aber jeder (Prim-)Teiler von $(n!)^2 + 1$ größer als n und eben $p \equiv 1 \bmod 4$.

Wäre der Teiler $p \equiv 3 \bmod 4$ so könnte eine Lösung für $x^2 \equiv -1 \bmod p$ gefunden werden mit $x = n!$. Leider kann es diese Lösung aber nicht geben da $\left(\frac{-1}{p}\right) = -1$ ist.

Bekannte Primzahlen

Bekannte Primzahlen

Zu den bekanntesten Primzahlen zählen die Primzahlen der Form:

$$2^n + 1 \text{ und } 2^n - 1$$

Wir betrachten nun welche Gestalt der Exponent haben muss, damit überhaupt eine Lösung existieren kann.

Mersennesche Primzahlen

Definition: *Zahlen der Gestalt*

$$M_n = 2^n - 1$$

heißen Mersennesche Zahlen. Sind Sie prim, spricht man von Mersenneschen Primzahlen.

Mersennesche Primzahlen

Notwendige Vorraussetzung:

Der Exponent ist eine Primzahl n=p. Währe der Exponent eine zusammengesetzte Zahl n=pq, so währe M_n durch $2^q - 1$ teilbar, da

$$\left(\frac{2^{pq}-1}{2^q-1}\right)=\left(\frac{(2^p)^q-1}{2^q-1}\right)=1+2^q+2^{2q}+\ldots+2^{(p-1)q}$$

damit die Lösung der Division gemäß der geometrischen Reihe liefert.

Mersennesche Primzahlen

Aufgabe:

Berechne die ersten 5 Mersennischen Zahlen aus den ersten 5 Primzahlen und machen Sie eine Aussage ob es sich um Mersennische Primzahlen handelt?

Mersennesche Primzahlen

Die ersten Mersenneschen Primzahlen sind:

p	M_n	Prim ?
2	3	Ja
3	7	Ja
5	31	Ja
7	127	Ja
11	2047	Nein

Bis heute sind 43 Mersennesche Primzahlen bekannt.

Fermatsche Primzahlen

Definition: *Zahlen der Gestalt*

$$F_n = 2^n + 1$$

heißen Fermatsche Zahlen. Eine Fermatsche Zahl die gleichzeitig Primzahl ist, wird Fermatsche Primzahl genannt.

Fermatsche Primzahlen

Notwendige Vorraussetzung:

Der Exponent ist eine Zweierpotenz $n = 2^k$. Währe der Exponent aus einem ungeraden Anteil n=g*u zusammengesetzte,so währe F_n durch $1+2^g$ teilbar, da

$$\left(\frac{1+2^{g\cdot u}}{1+2^g}\right) = \left(\frac{1-(-2^g)^u}{1-(-2^g)}\right) = 1+(-2^g)+(-2^g)^2+\ldots+(-2^g)^{(u-1)}$$

damit die Lösung der Division gemäss der geometrischen Reihe liefert.

Fermatsche Primzahlen

Die ersten Fermatschen Primzahlen sind:

k	F_p	Prim?
0	3	Ja
1	5	Ja
2	17	Ja
3	257	Ja
4	65537	Ja
5	4.294.967.297	Nein

Bis heute sind keine weiteren Fermatschen Primzahlen bekannt.

Teilbarkeitsregeln

Bekannte Sätze der Teilbarkeitsregeln lassen sich mit Hilfe der Zahlentheorie bewältigen:

Wann ist eine Zahl durch 3, 9 oder 11 teilbar?

Betrachten wir hierzu zunächst die Zerlegung der Zahl in das Zehnersystem. Jede (k+1)-stellige Zahl hat eine eindeutige Darstellung:

$$n = \sum_{i=0}^{k} a_i \cdot 10^i$$

Teilbarkeitsregeln

Wir betrachten die Teilbarkeit durch 3:

$$n \equiv 0 \bmod 3$$

Da aber

$$1 \equiv 1 \bmod 3 \quad \text{und}$$

$$10 \equiv 1 \bmod 3$$

ist auch

$$10^i \equiv 1 \bmod 3 \quad \text{und}$$

$$a_i \cdot 10^i \equiv 1 \cdot a_i \bmod 3$$

Teilbarkeitsregeln

$$n = \sum_{i=0}^{k} (a_i \cdot 10^i) \equiv (\sum_{i=0}^{k} a_i) \bmod 3$$

Damit gilt:

$$n \equiv 0 \bmod 3 \Leftrightarrow \sum_{i=0}^{k} a_i \equiv 0 \bmod 3$$

Dies Bedeutet: Eine Zahl ist genau dann durch 3 teilbar, wenn die Summe ihrer Ziffern(also die Quersumme) durch 3 teilbar ist

Teilbarkeitsregeln

Aufgabe:

Führen Sie nach gleichem Prinzip den Beweis für die Teilbarkeit durch 9 durch:

Teilbarkeitsregeln

Teilbarkeit durch 11:

$$n \equiv 0 \bmod 11$$

Da aber

$$1 \equiv 1 \bmod 11$$

$$10 \equiv -1 \bmod 11$$

$$10^2 = 100 \equiv 1 \bmod 11$$

ist auch

$$10^i \equiv (-1)^i \bmod 11$$

Teilbarkeitsregeln

und

$$a_i \cdot 10^i \equiv a_i \cdot (-1)^i \bmod 11$$

$$n = \sum_{i=0}^{k} (a_i \cdot 10^i) \equiv (\sum_{i=0}^{k} a_i \cdot (-1)^i) \bmod 11$$

Damit gilt

$$n \equiv 0 \bmod 11 \Leftrightarrow \sum_{i=0}^{k} (a_i \cdot (-1)^i) \equiv 0 \bmod 11$$

Teilbarkeitsregeln

Dies bedeutet: Eine Zahl ist genau dann durch 11 teilbar, wenn die alternierende Summe ihrer Ziffer (also die alternierende Quersumme) durch 11 teilbar ist.

Beispiel: 53967432607 durch 11 teilbar?

Alternierende Summe: 5-3+9-6+7-4+3-2+6-0+7=22. Da diese Zahl durch 11 teilbar ist, ist damit auch die ursprüngliche Zahl durch 11 Teilbar.