Kryptologie, SS03 Aufgabenblatt 4

Quadratische Reste, Legendre- und Jacobi-Symbol

Sei $p \geq 3$ eine Primzahl. Betrachtet man in $\mathbb{Z}_p^*$ die Abbildung $x \to x^2$, so kommt genau die Hälfte der Elemente von $\mathbb{Z}_p^*$ als Bilder vor. Gibt es für ein $a \in \mathbb{Z}_p^*$ ein $b \in \mathbb{Z}_p^*$ mit $b^2 = a$, so ist offenbar auch $(-b)^2 = a$; jedes zweite Element von $\mathbb{Z}_p^*$ ist ein „Quadrat modulo *p*" und besitzt 2 „Quadratwurzeln", die andere Hälfte der Elemente von $\mathbb{Z}_p^*$ besitzt keine Quadratwurzel.

Man setzt nun für $a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) := \begin{cases} 1, \text{ falls } (a\% p) \neq 0 \text{ Quadrat in } \mathbb{Z}_p^* \text{ ist} \\ -1, \text{ falls } (a\% p) \neq 0 \text{ kein Quadrat in } \mathbb{Z}_p^* \text{ ist} \\ 0, \text{ falls } (a\% p) = 0 \end{cases}$$

$\left(\frac{a}{p}\right)$ heißt „Legendre-Symbol" von „*a* nach *p*".

Es gelten folgende Rechenregeln: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, $\left(\frac{a}{p}\right) = \left(\frac{a\% p}{p}\right)$ und $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Um das Legendre Symbol berechnen und damit feststellen zu können, ob ein Element von $\mathbb{Z}_p^*$ ein Quadrat in $\mathbb{Z}_p^*$ ist, benötigen wir das „Jacobi-Symbol". Ist $n \in \mathbb{N},\ n \geq 3,\ n$ ungerade und $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ die Primzahlzerlegung von *n*, so setzen wir

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

Ist n eine Primzahl, so fallen offenbar die Begriffe „Jacobi-Symbol" und „Legendre Symbol" zusammen. Zur Berechnung des Jacobi-Symbols, damit auch des Legendre-Symbols, und damit zur Entscheidung, ob ein Element von $\mathbb{Z}_p^*$ ein Quadrat in $\mathbb{Z}_p^*$ ist, braucht man folgende Eigenschaften des Jacobi Symbols:

Sind $n, m \in \mathbb{N},\ n, m \geq 3,\ n, m$ ungerade, $a, b \in \mathbb{Z}$.

i) $\left(\frac{a}{n}\right) \in \{-1, 0, 1\}$; $\left(\frac{a}{n}\right) = 0 \Leftrightarrow \mathrm{ggT}(a, n) \neq 1$

ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$. Also gilt für $a \in \mathbb{Z}$: $\left(\frac{a^2}{n}\right) = 1$.

iii) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

iv) Wenn $a \equiv b \bmod n$, dann $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

v) $\left(\frac{1}{n}\right)=1,\ \left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}},\ \left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$

Man beachte, daß $\frac{n-1}{2}$ genau dann gerade ist, wenn die Dualzahldarstellung von *n* mit 01 aufhört, und daß $\frac{n^2-1}{8}$ genau dann gerade ist, wenn die Dualzahldarstellung von *n* mit 001 oder 111 aufhört.

vi) $\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$ (das sog. „quadratische Reziprozitätsgesetz“)

$\frac{(m-1)(n-1)}{4}$ ist genau dann ungerade, wenn die Dualzahldarstellungen von *m,n* beide mit 11 aufhören.

Mit Hilfe dieser Rechenregeln ergibt sich folgender Pseudo-Code zur Berechnung des Jacobi-Symbols:

Jacobi(a,n)
Input: $n \in \mathbb{N}, n \geq 3, n$ ungerade, $a \in \mathbb{Z}$
Output: das Jacobi Symbol $\left(\frac{a}{n}\right)$ und damit das Legendre Symbol, falls *n* prim

1. Wenn a=0, dann **return**(0)
2. Wenn a=1, dann **return**(1)
3. Schreibe $a = 2^s u$, *u* ungerade
4. Wenn *s* gerade oder wenn $n\%8 \in \{1,7\}$, dann setze $t \leftarrow 1$; sonst setze $t \leftarrow -1$
5. Wenn $u\%4 = 3$ und $n\%4 = 3$, dann setze $t \leftarrow -t$
6. Setze $n_1 \leftarrow n\%u$
7. **return**($t \cdot$ **Jacobi**(n_1, u))

Aufgabe 1

a) Stelle „per Hand“ fest, ob die Gleichung $x^2 = 3$ in $\mathbb{Z}_{3001}$ eine Lösung besitzt.

b) Programmiere obigen Algorithmus und stelle fest, ob die Gleichung $x^2 = 363495$ in $\mathbb{Z}_{316058881}$ eine Lösung besitzt.

Aufgabe 2

Miller Rabin Primzahltest

Sei *n* eine ungerade Primzahl, $n-1 = 2^s u$, *u* ungerade und $a \in \mathbb{Z}_n^*$. Dann ist entweder $a^u = 1$ in $\mathbb{Z}_n^*$ oder $a^{2^k u} = -1$ in $\mathbb{Z}_n^*$ für ein *k*<*s*. Bildet man also ausgehend von $x_1 := x^u$ in $\mathbb{Z}_n^*$ durch wiederholtes Quadrieren die Folge $x_{n+1} := x_n{}^2$, so ist $x_1 = 1$ oder es wird $x_k = -1$ für *k*<*s*.

Um mit Hilfe dieser Fakten einen Algorithmus zu formulieren, wähle man zunächst einen „Sicherheitsparameter“ *t*, Die Wahrscheinlichkeit, daß der Algorithmus eine Nicht-Primzahl zur Primzahl erklärt, ist dann $\frac{1}{4^t}$. Wird dagegen eine Zahl als Nicht-Primzahl erkannt, so ist dieses Ergebnis sicher.

Isprime_Miller-Rabin(*n*,*t*)
Input: $n \in \mathbb{N}, n \geq 3, \text{n ungerade}$, $t \in \mathbb{N}$
Output: wahr oder falsch

1. Schreibe $n-1=2^s u$, u ungerade
2. Durchlaufe *t*-mal folgende Schleife{
   - 2.1 Wähle eine Zufallszahl $a \in \mathbb{N}, 2 \leq a \leq n-2$
   - 2.2 Berechne $y=a^r$ in $\mathbb{Z}_n$ (durch wiederholtes Quadrieren, wie gehabt)
   - 2.3 Wenn $y \neq 1$ oder $y \neq n-1$, dann {
     - 2.3.1 Durchlaufe (*s*-1) mal folgende Schleife {
       - 2.3.1.1 $y \leftarrow y^2 \bmod n$
       - 2.3.1.2 Wenn (*y*=1), dann **return**(falsch)
       - 2.3.1.3 Wenn (*y*=*n*-1) dann **goto** 2.

       }

     }

   }
3. **return**(wahr)

Aufgabe 3

a) Man wähle zwei zufällige Primzahlen $2^{511} \leq p, q \leq 2^{512}$, setze *n:=pq*, wähle einen zufälligen Startwert $s \in \mathbb{Z}_n^*$, berechne in $\mathbb{Z}_n^*$ $x_1 := s^2$ und $x_{n+1} := x_n{}^2$ und erzeuge so eine Bytefolge b_n, indem man jeweils das niedrigstwertige Byte von x_n nimmt.
(Blum-Blum-Shub Zufallsgenerator)
Mit der b_n entsprechenden Bitfolge färbe man die Folge der Pixel eines Computerbildschirms schwarz bzw. weiß, je nach Bitwert des betreffenden Bitfolgenglieds. (Oder man ordne jeweils 3 Byte der Folge b_n den rgb-Farbwerten des jeweiligen Pixels zu, um ein farbiges Bild zu erhalten.) Können Sie Muster erkennen?

b)*
Wir denken uns die Pixel eines Computerbildschirms beschrieben durch Bitwerte $b_{i,j}$, wobei *i* die Pixelzeile und *j* die Spalte zählt. Man wähle jetzt zwei Zahlen *a*,*b*, z.B. $a=1234567$ und $b=7654321$, und setze $b_{i,j} := k-$tes Bit der Dualzahldarstellung von $(a+i)^2+(b+j)^2$
Für welche *k* erhält man die interessantesten Bilder?