und hierfür gilt $b \in E(m) \setminus A(m)$.

(2) Es sei $m \geq 3$ eine ungerade natürliche Zahl, die keine Primzahl ist. Dann ist nach (1) $A(m)$ eine echte Teilmenge von $E(m)$. Man zeige, daß

$$\{[a]_m \mid a \in A(m)\}$$

eine Untergruppe der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ ist, und folgere daraus: Es gilt

$$\#(A(m)) \leq \frac{1}{2}\#(E(m)).$$

(3) Man formuliere mit Hilfe von (1) und (2) einen stochastischen Primzahltest; dabei orientiere man sich an dem Algorithmus RABIN in (7.5). Man schreibe dazu eine MuPAD-Funktion.

Bemerkung: Leider ist der Primzahltest von Solovay und Strassen nicht dazu geeignet, den Primzahltest von Rabin zu ergänzen: Ist m eine starke Pseudoprimzahl zu einer Basis $b \in \mathbb{N}$, so liegt $b \bmod m$ in der Menge

$$A(m) = \left\{a \in E(m) \,\middle|\, a^{(m-1)/2} \equiv \left(\frac{a}{m}\right) \pmod{m}\right\}.$$

(Zum Beweis vergleiche man Koblitz [57], V, § 1). Wenn also der Primzahltest von Rabin eine Nichtprimzahl m als Primzahl deklariert, so tut dies auch der Primzahltest von Solovay und Strassen, falls in beiden Tests dieselben Zufallszahlen verwendet werden.

12 Ein Rechenverfahren

(12.1) In diesem Paragraphen wird die Aufgabe gelöst, zu einer ungeraden Primzahl p und zu einem quadratischen Rest $a \in \mathbb{Z}$ modulo p eine ganze Zahl x mit $x^2 \equiv a \pmod{p}$ zu berechnen. Einen Algorithmus, der dieses leistet, gab D. Shanks 1972 in [103] an; er nannte ihn RESSOL (= RESidue SOLver). Einen Vorläufer dieses Algorithmus publizierte A. Tonelli bereits im Jahr 1891 in [108]. Der Algorithmus RESSOL benötigt einen quadratischen Nichtrest z modulo der Primzahl p, auf die er angewandt wird. Daher muß man sich zuerst überlegen, wie man ein solches z findet.

(12.2) Satz: *Es sei p eine ungerade Primzahl, und es sei $z(p)$ der kleinste positive quadratische Nichtrest modulo p. Es gilt*

$$z(p) < 1 + \sqrt{p}.$$

Beweis: Für $z := z(p)$ gilt $2 \leq z \leq p-1$. Für $k := \lceil p/z \rceil$ gilt $k-1 < p/z \leq k$, wegen $p/z > 1$ ist daher $k \geq 2$, und es ist $p/z < k$, denn sonst wäre $p = zk$.

F. Schwarz, *Einführung in die Elementare Zahlentheorie*

Wegen $k-1 < p/z < k$ gilt $1 \leq kz - p < z \leq p-1$, und daher ist $kz-p$ ein quadratischer Rest modulo p. Es gilt also

$$1 \;=\; \left(\frac{kz-p}{p}\right) \overset{(11.4)(1)}{=} \left(\frac{kz}{p}\right) \overset{(11.4)(2)}{=} \left(\frac{k}{p}\right)\left(\frac{z}{p}\right) \;=\; -\left(\frac{k}{p}\right),$$

k ist somit ein quadratischer Nichtrest modulo p, und daher ist $z \leq k$. Also ist

$$(z-1)^2 \;<\; (z-1)z \;\leq\; (k-1)z \;<\; p,$$

und daher gilt $z < 1 + \sqrt{p}$.

(12.3) Bemerkung: (1) Es sei für jede ungerade Primzahl p wie in (12.2) $z(p)$ der kleinste positive quadratische Nichtrest modulo p. Die Abschätzung in (12.2) ist sehr pessimistisch. In Wirklichkeit kann man viel mehr beweisen: D. Burgess zeigte in [18], daß es zu jedem reellen $\varepsilon > 0$ ein $N_0(\varepsilon) \in \mathbb{N}$ mit der folgenden Eigenschaft gibt: Für jede Primzahl $p > N_0(\varepsilon)$ gilt $z(p) < p^{a+\varepsilon}$, wobei $a = 1/(4\sqrt{e}) = 0.151\,632\ldots$ ist (vgl. Narkiewicz [73], Kap. II, §1). Unter der Voraussetzung, daß die verallgemeinerte Riemannsche Vermutung (vgl. (5.5) und (7.4)) richtig ist, ergibt sich auch hier ein besseres Ergebnis: Für jede ungerade Primzahl p gilt $z(p) < 2(\log p)^2$ (dazu vgl. man die Dissertation [8] von E. Bach). Auf der anderen Seite gibt es ein reelles $c > 0$ mit: Für unendlich viele Primzahlen p ist $z(p) > c \log p$ (vgl. dazu Salié [96]).
(2) Zur Berechnung des kleinsten positiven quadratischen Nichtrests $z(p)$ zu einer ungeraden Primzahl p kennt man keinen effizienten Algorithmus. Falls die verallgemeinerte Riemannsche Vermutung richtig ist, führt das folgende Verfahren in vernünftiger Zeit zum Ziel:

```
z := 2; while numlib::jacobi(z,p) = 1 do z := z + 1 end_for;
```

Dies zeigt auch die Praxis, jedenfalls für kleine Primzahlen, denn mit etwas Geduld kann man mittels MuPAD nachrechnen: Es gilt

$$\begin{aligned}
\max\big(\{z(p) \mid p \text{ Primzahl; } p < 1\,000\,000\}\big) &= z(366\,791) = 43,\\
\max\big(\{z(p) \mid p \text{ Primzahl; } p < 10\,000\,000\}\big) &= z(9\,257\,329) = 53,\\
\max\big(\{z(p) \mid p \text{ Primzahl; } p < 100\,000\,000\}\big) &= z(48\,473\,881) = 67,\\
\max\big(\{z(p) \mid p \text{ Primzahl; } p < 1\,000\,000\,000\}\big) &= z(131\,486\,759) = 83.
\end{aligned}$$

(12.4) Hilfssatz: *Es sei p eine Primzahl, es seien $b, c \in \mathbb{Z} \setminus p\mathbb{Z}$, und es gelte* $\operatorname{ord}([b]_p) = 2^\beta = \operatorname{ord}([c]_p)$ *mit einem $\beta \in \mathbb{N}$. Es gibt ein $\gamma \in \{0,1,\ldots,\beta-1\}$ mit*

$$\operatorname{ord}([bc]_p) \;=\; 2^\gamma.$$

Beweis: Im Körper $\mathbb{F}_p$ gilt

$$[0]_p = [b]_p^{2^\beta} - [1]_p = \left([b]_p^{2^{\beta-1}} - [1]_p\right)\left([b]_p^{2^{\beta-1}} + [1]_p\right),$$

wegen $\operatorname{ord}([b]_p) = 2^\beta$ gilt $[b]_p^{2^{\beta-1}} \neq [1]_p$, und daher ist

$$[b]_p^{2^{\beta-1}} = -[1]_p = [-1]_p.$$

Ebenso ergibt sich $[c]_p^{2^{\beta-1}} = [-1]_p$. Also gilt

$$[bc]_p^{2^{\beta-1}} = [b]_p^{2^{\beta-1}} \cdot [c]_p^{2^{\beta-1}} = [-1]_p \cdot [-1]_p = [1]_p,$$

und daher ist die Ordnung von $[bc]_p$ in der Gruppe $\mathbb{F}_p^\times$ ein Teiler von $2^{\beta-1}$ [vgl. (3.5)(3)]. Also gibt es ein $\gamma \in \{0, 1, \ldots, \beta-1\}$ mit $\operatorname{ord}([bc]_p) = 2^\gamma$.

(12.5) Der Algorithmus RESSOL: Es sei p eine ungerade Primzahl, und es sei $a \in \mathbb{Z}$ ein quadratischer Rest modulo p. Der Algorithmus berechnet ein $x \in \{0, 1, \ldots, p-1\}$ mit $x^2 \equiv a \pmod p$.

> **(RESSOL 1)** Ist $p \equiv 3 \pmod 4$, so setzt man
>
> $$x := a^{(p+1)/4} \bmod p,$$
>
> gibt x aus, und bricht ab.

Bemerkung: Ist $p \equiv 3 \pmod 4$, so ist $p+1$ durch 4 teilbar, und es gilt

$$0 \leq x = a^{(p+1)/4} \bmod p \leq p-1$$

und

$$x^2 \equiv a^{(p+1)/2} = a^{(p-1)/2} \cdot a \overset{(11.3)}{\equiv} 1 \cdot a = a \pmod p.$$

> **(RESSOL 2)** Man ermittelt wie in (12.3)(2) einen quadratischen Nichtrest z modulo p.

> **(RESSOL 3)** Man setzt
>
> $$\alpha := v_2(p-1) \quad \text{und} \quad m := (p-1)/2^\alpha.$$

Bemerkung: Es gilt $\alpha \geq 2$, m ist ungerade, und es ist $p - 1 = 2^\alpha m$.

> **(RESSOL 4)** Man setzt
>
> $$w := z^m \bmod p, \quad x := a^{(m+1)/2} \bmod p, \quad y := a^m \bmod p.$$

Bemerkung: (a) Es gilt $x^2 \equiv a^{m+1} \equiv ay \pmod{p}$.
(b) Ist $y = 1$, so gilt $x^2 \equiv a \pmod{p}$.
(c) Es gelte $y \neq 1$. Es gilt $p \nmid w$, wegen

$$w^{2^\alpha} \equiv z^{2^\alpha m} = z^{p-1} \overset{(4.21)(1)}{\equiv} 1 \pmod{p}$$

ist $\operatorname{ord}([\,w\,]_p)$ ein Teiler von 2^α, und wegen

$$w^{2^{\alpha-1}} \equiv z^{2^{\alpha-1} m} = z^{(p-1)/2} \overset{(11.3)}{\equiv} -1 \not\equiv 1 \pmod{p}$$

gilt daher $\operatorname{ord}([\,w\,]_p) = 2^\alpha$. Es gilt $p \nmid y$ und $y \not\equiv 1 \pmod{p}$ und

$$y^{2^{\alpha-1}} \equiv a^{2^{\alpha-1} m} = a^{(p-1)/2} \overset{(11.3)}{\equiv} 1 \pmod{p},$$

und daher gibt es ein $\beta \in \{1, 2, \ldots, \alpha - 1\}$ mit $\operatorname{ord}([\,y\,]_p) = 2^\beta$.

> **(RESSOL 5)** Ist $y = 1$, so gibt man x aus und bricht ab.

> **(RESSOL 6)** Man bestimmt die Zahl β mit $\operatorname{ord}([\,y\,]_p) = 2^\beta$.

Bemerkung: β ermittelt man so:

```
beta := 1;
temp := y^2 mod p;
while temp <> 1 do
  beta := beta + 1;
  temp := temp^2 mod p
end_while;
```

> **(RESSOL 7)** Man setzt
>
> $$v := w^{2^{\alpha-\beta-1}} \bmod p, \quad w' := v^2 \bmod p,$$
> $$x' := vx \bmod p, \quad y' := w'y \bmod p.$$

Bemerkung: (a) Es gilt $x'^2 \equiv v^2x^2 \equiv w'ay \equiv ay' \pmod{p}$.
(b) Es gilt

$$\begin{aligned} \operatorname{ord}([w']_p) &= \operatorname{ord}([w^{2^{\alpha-\beta}}]_p) = \operatorname{ord}([w]_p^{2^{\alpha-\beta}}) = \\ &\overset{(3.7)(2)}{=} \frac{\operatorname{ord}([w]_p)}{\operatorname{ggT}(2^{\alpha-\beta}, \operatorname{ord}([w]_p))} = \frac{2^\alpha}{\operatorname{ggT}(2^{\alpha-\beta}, 2^\alpha)} = \\ &= \frac{2^\alpha}{2^{\alpha-\beta}} = 2^\beta = \operatorname{ord}([y]_p) > 1, \end{aligned}$$

also gibt es nach (12.4) ein $\gamma \in \{0, 1, \ldots, \beta - 1\}$ mit

$$\operatorname{ord}([y']_p) = \operatorname{ord}([w']_p \cdot [y]_p) = 2^\gamma,$$

und daher ist $\operatorname{ord}([y']_p) = 2^\gamma < 2^\beta = \operatorname{ord}([y]_p)$.

> **(RESSOL 8)** Man setzt
>
> $$w := w', \quad x := x', \quad y := y' \quad \text{und} \quad \alpha := \beta$$
>
> und geht zu (RESSOL 5).

Bemerkung: (a) Vor dem Eintritt in (RESSOL 5) gilt stets

$$x^2 \equiv ay \pmod{p} \quad \text{und} \quad \operatorname{ord}([y]_p) < \operatorname{ord}([w]_p).$$

(b) Sind y_1, y_2, $y_3, \ldots$ die nacheinander berechneten Werte von y, so gilt

$$\operatorname{ord}([y_1]_p) > \operatorname{ord}([y_2]_p) > \operatorname{ord}([y_3]_p) > \cdots \geq 1$$

(vgl. die Bemerkung vor (RESSOL 8)), also nimmt y nach endlich vielen Schritten den Wert 1 an, und das Verfahren bricht in (RESSOL 5) ab. Damit ist gezeigt, daß der Algorithmus RESSOL das Verlangte leistet.

(12.6) MuPAD: Die Funktion `numlib::msqrts` liefert zu einer natürlichen Zahl m und einer ganzen Zahl a mit $\operatorname{ggT}(a, m) = 1$ die Liste der der Größe nach geordneten Zahlen $x \in \{0, 1, \ldots, m-1\}$ mit $x^2 \equiv a \pmod{m}$, falls a ein quadratischer Rest modulo m ist, und andernfalls die Ausgabe `FAIL`.

```
>> p := 131486759: isprime(p);
                                    TRUE
>> numlib::msqrts(1998,p);
                          [17944220,113542539]
```

```
>> q := nextprime(1997199719971997199719971997);
              1997199719971997199719972139
>> numlib::msqrts(1998,q);
   [9562778243243369354603690602362,
                        10409218956476602642596029369777]
>> numlib::msqrts(1998,p*q);
   [229733179959817947213766394309292094558,
        270711205388716906271582140547746386559,
            2355341977159537919210966114296381020942,
                2396320002588436878268781860534835312943]
```

(12.7) Aufgaben:

Aufgabe 1: Man schreibe eine MuPAD-Funktion `ressol` für den Algorithmus RESSOL aus (12.5).

Aufgabe 2: Man schreibe eine MuPAD-Funktion, die wie die Funktion `numlib::msqrts` zu einer natürlichen Zahl m und einer zu m teilerfremden ganzen Zahl a die Lösungen $x \in \{0, 1, \ldots, m-1\}$ von $X^2 \equiv a \pmod m$ berechnet, falls a ein quadratischer Rest modulo m ist, und andernfalls die Ausgabe `FAIL` liefert. Diese Funktion sollte dabei die Funktion `ressol` aus Aufgabe 1 verwenden.