Übungen zur Vorlesung Computeralgebra (Blatt 3)

PD Dr. Jürgen Müller

(3.1) Aufgabe: Modulare Arithmetik.

a) Für $n \geq 2$ sei $\mathbb{Z}_n := \{0, \ldots, n-1\} \subseteq \mathbb{Z}$, und für $a \in \mathbb{Z}$ sei $\overline{a} \in \mathbb{Z}_n$ der Rest der Division von a durch n. Zeigen Sie (in Ihrem Arbeitsheft), die folgende Eigenschaft: Sind $a, a', b, b' \in \mathbb{Z}$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, so gilt auch $\overline{a+b} = \overline{a'+b'}$ und $\overline{ab} = \overline{a'b'}$. Folgern Sie daraus, daß die modulare Addition und Multiplikation die Assoziativ- und Distributivgesetze erfüllen.

b) Implementieren Sie SAGE-Funktionen, etwa `add(a,b,n)`, `mult(a,b,n)` und `inv(a,n)`, zur modularen Addition, Multiplikation, und zur Berechnung eines modularen Inversen (sofern eines existiert). Verwenden Sie zur Bestimmung modularer Inverser Ihre Implementation des (erweiterten) Euklidischen Algorithmus.

Man bestimme alle $a \in \mathbb{N}_0$ mit $a < 1000$, so daß $67a$ in Dezimaldarstellung die drei letzten Ziffern 123 hat. Was passiert, wenn man stattdessen $68a$ und/oder 124 betrachtet?

c)* Es sei $\mathbb{Z}_n^*$ die Einheitengruppe von $\mathbb{Z}_n$. Zeigen Sie (in Ihrem Arbeitsheft), daß $1 \in \mathbb{Z}_n^*$ das einzige neutrale Element ist, und daß jedes Element von $\mathbb{Z}_n^*$ ein eindeutig bestimmtes inverses Element besitzt.

Untersuchen Sie die Werte $\varphi(n) = |\mathbb{Z}_n^*|$ der Eulerschen φ-Funktion für einige $n \in \mathbb{N}$, und versuchen Sie, Gesetzmäßigkeiten zu entdecken.

(3.2) Aufgabe: Exponentiation.

a) Führen Sie den 'Repeated-Squaring'-Algorithmus zur modularen Exponentiation (in Ihrem Arbeitsheft) für das Beispiel $n := 17$, $a := 8$ und $e := 13$ aus

b) Implementieren Sie eine SAGE-Funktion, etwa `pow(a,e,n)`, zur Berechnung von $a^e \in \mathbb{Z}_n$, wobei $n \geq 2$, $a \in \mathbb{Z}_n$ und $e \in \mathbb{N}$, die den 'Repeated-Squaring'-Algorithmus benutzt. Achten Sie dabei wiederum darauf, welche Variablen benötigt werden; insbesondere sollte die Binärdarstellung des Exponenten $e \in \mathbb{N}$ nicht explizit berechnet werden.

Vergleichen Sie, für einige selbstgewählte (große) Beispiele, die Ergebnisse und Laufzeiten Ihrer Implementation mit dem herkömmlichen SAGE-Aufruf '$(a\hat{}e)\%n$'.

c)* Für $n \in \mathbb{N}_0$ sei $F_n := 2^{2^n} + 1 \in \mathbb{N}$ die n-te **Fermat-Zahl**. Es fällt auf, daß $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sämtlich Primzahlen sind, was [Fermat, 1640] veranlaßte, zu vermuten, daß alle Fermat-Zahlen prim sind. Aber nach [Euler, 1732] ist $F_5 = 4\,294\,967\,297$ nicht prim: Zeigen Sie (in Ihrem Arbeitsheft), daß $641 \mid F_5$ gilt; verifizieren Sie das auch mittels Ihrer obigen SAGE-Funktion.

(3.3) Aufgabe: RSA-Cryptosystem mit Signatur.
a) Wählen Sie einen RSA-Modulus $n := pq < 10^{100}$, wobei $p \neq q$ Primzahlen sind; richten Sie es so ein, daß n nicht in handhabbarer Zeit mittels der SAGE-Funktion factor faktorisiert werden kann. (Wir hatten ja schon in Aufgabe (2.3)(d) gesehen, daß es reichlich große Primzahlen gibt, diese sind also leicht zu finden; beachten Sie dazu die SAGE-Funktion next_prime.)

Wählen Sie weiter einen öffentlichen RSA-Schlüssel $e \in \mathbb{Z}_n$, und bestimmen Sie einen zugehörigen geheimen Schlüssel $d \in \mathbb{Z}_n$; richten Sie es so ein, daß d nicht leicht aus n und e allein berechnet werden kann.

b) Ziel ist es nun, eine verschlüsselte Nachricht zu senden, und diese gleichzeitig zu authentifizieren. Führen Sie dazu folgendes Signatur-Protokoll aus:

• Wählen Sie die Nachricht $a := m^i$, wobei $m \in \mathbb{N}$ Ihre Matrikelnummer und $i := \lfloor \log_m(n) \rfloor \in \mathbb{N}$ sind. (Eigentlich soll die gesendete Nachricht ja nicht öffentlich bekannt, sondern nur für den Empfänger zu entschlüsseln sein, aber hier dient das natürlich dazu, die Korrektheit Ihrer RSA-Implementation zu überprüfen.)

• Verschlüsseln Sie $a \in \mathbb{Z}_n$ zunächst mittels Ihres geheimen Schlüssels d, danach verschlüsseln Sie das Ergebnis $b \in \mathbb{Z}_n \subseteq \mathbb{Z}_N$ mit unserem unten genannten öffentlichen Schlüssel E. Senden Sie uns das Ergebnis $c \in \mathbb{Z}_N$ (in Ihrer E-Mail-Abgabe), zusammen mit Ihrem Modulus n und Ihrem öffentlichen Schlüssel e. (Wenn Sie gemeinschaftlich abgeben, so führen Sie das für alle Ihre Matrikelnummern aus; dabei brauchen Sie natürlich n und e nur einmal zu wählen.)

Hier unser öffentlicher Schlüssel: Wir wählen $E := 2^{16} + 1 = 65537$, und N ist die folgende 101-stellige Zahl: (Der Modulus steht auch als Text-Datei zur Verfügung.)

164201572649746711693859559321745062306256253080626
96691855505073410692113405870505702894013562132361

c) Überlegen Sie sich (in Ihrem Arbeitsheft), wie aus den gesendeten Informationen die Nachricht zurückgewonnen werden kann, und wieso es sich gleichzeitig um eine Signatur handelt.

Protokollieren Sie wie üblich Ihre Rechnungen in einer '.txt'-Datei, in die Sie auch Ihre '.sage'-Datei kopieren.

Abgabe per E-Mail an abgabe-compalg@math.uni-hannover.de bis spätestens Montag, den 03.12.2012, 16:00 Uhr. Gemeinschaftsabgabe ist bis zu drei Personen zulässig, unter Betreff Blatt 3, Matrikelnummer1, Matrikelnummer2, Matrikelnummer3.