Mathematisches Institut
der Universität München
Pascal Reisert

Wintersemester 2015/2016
Übungsblatt 7
09. Dezember 2015

Übungen zur Algorithmischen Zahlentheorie
Lösung

Aufgabe 26

a) Der folgende Beweis beruht auf der Lösung von *Ludwig Fürst*: Sei a zunächst ungerade. Wir sehen sofort, dass $\left(\frac{p}{a}\right) = \left(\frac{q}{a}\right)$ gilt. Sei $p - q = 4da, d \in \mathbb{Z}$. Da $a(a-1)$ gerade ist, folgt mit

$$\left(\frac{q}{a}\right) = (-1)^{da(a-1)}\left(\frac{p}{a}\right) = (-1)^{(4da(a-1))/4}\left(\frac{p}{a}\right) = (-1)^{(p-1-q+1)(a-1)/4}\left(\frac{p}{a}\right)$$
$$\Rightarrow (-1)^{(q-1)(a-1)/4}\left(\frac{q}{a}\right) = (-1)^{(p-1)(a-1)/4}\left(\frac{p}{a}\right) \Rightarrow \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$$

die Aussage.
Ist a gerade so gilt $a = 2^k b$ mit einer ungeraden Zahl b, $k \geqslant 1$. Dann gilt $8 \mid 4a$ und somit auch $p \equiv q \bmod 8$ sowie nach dem zweiten Ergänzungssatz $\left(\frac{2}{p}\right)^k = \left(\frac{2}{q}\right)^k$. Somit folgt aus dem ungeraden Fall auch

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^k\left(\frac{b}{p}\right) = \left(\frac{2}{q}\right)^k\left(\frac{b}{q}\right) = \left(\frac{a}{q}\right).$$

Aufgabe 28

Mit `qs_factorize` erhalten wir

```
N=pq,
p=1_26727_50579_18552_39745_55977_48763,
q=84661_13346_19447_78737_55126_49519.
```

Wir kennen bereits die Zahl

```
z_{896}
:=0x30_BD73_ B0D0_9953_2BAD_B86B_59B0_A97E_2727_CE2B_AA0D_9A86_4947
=30594_62307_80124_54064_86824_79292_97916_68740_78591_54082_02610_95751.
```

Sei a gegeben und gesucht sei ein x mit $x^2 = a \bmod N$. Angenommen wir finden einen Lösung x_p mit $x_p^2 = a \bmod p$ und eine Lösung x_q mit $x_q^2 = a \bmod q$. Dann können wir eine Lösung x wie folgt konstruieren. Sei $bp + cq = 1$, dann ist $x = x_p \cdot c \cdot q + x_q \cdot b \cdot p$ eine Lösung von $x^2 = a \bmod N$:

$$x^2 \bmod N = x_p^2c^2q^2 + x_q^2b^2p^2 \bmod N = ac^2q^2 + ab^2p^2 \bmod N$$
$$= a + 2apb(bp-1) \bmod N = a \bmod N.$$

Für die Primzahlen p, q finden wir aber wie in Aufgabe 27 Lösungen der Gleichung $x^2 = a \bmod p$ reps. $x^2 = a \bmod q$. Sei $p = 3 \bmod 4$ und $\left(\frac{a}{p}\right) = 1$, dann gilt für $x = a^{(p+1)/4}$

$$x^2 = a^{(p+1)/2} = aa^{(p-1)/2} = a \bmod p.$$

Als `aribas`-Funktion kann dies z.B. wie folgt realisiert werden:

```
function rroot(y,p:integer): integer;
begin
if p mod 4= 3 then y:=y**((p+1) div 4) mod p;
return y;
else writeln("invalid p");
halt;
end;
end.
```

b und c mit $bp + cq = 1$ lässt sich in `aribas` mittels der Funktion `gcd_coeff` (siehe §4 des Buches von Prof. Forster bestimmen).

```
function gcd_coeff(x,y,integer):array[3];
var
q, temp, q11, q12, q21, q22, t21, t22: integer;
begin
q11 := q22 := 1; q12 :=  q21 := 0;
while y /= 0 do
temp := y;
q := x div y;
y := x mod y;
x := temp;
t21 := q21; t22 := q22;
q21 := q11 - q*q21;
q22 := q12 - q*q22;
q11 := t21; q12 := t22;
end;
return(x,q11,q12);
end.
```

Es folgt

```
b:=-31848_65740_82423_33821_75746_35820,
c:=47673_59886_55298_71524_71014_34219.
```

Nun können wir z_0 berechnen mittels

```
function calcz0(y:integer):integer;
external
p,q,b,c,N;
var
k:integer;
begin
for k:=1 to 896 do;
y:=(rroot(y,p)*c*q+rroot(y,q)*b*p) mod N;
end;
return y;
end.
```

und

```
z_0:=15862_07536_52593_39020_72231_21342_74620_78114_95881_44189_21077_18047
```

Der verschlüsselte Text

```
CC:=EAD3_99D0_4DF9_96AE_31D6_1D2B_CC32_63A6_CD4F_C77D_4D5C_C3C2_6D57_353D_
0B16_E50F_8821_A2E9_19A6_3AFF_0718_366E_D3FF_95DE_C9EE_42E5_24D3_3370_
E37C_AC2A_3305_B45B_E691_5EAE_8ED7_046F_8A77_3AB3_CF18_A1E4_42C3_1FF3_
C53D_30CB_CE28_2684_24E3_2835_9C83_0C6B_BC65_8FFA_7B3C_9130_D24B_A8BC
```

kann nur mittels

```
function go28(y:integer):byte_string;
external
N,CC;
var
k:integer;
bb: byte_string[112];
begin
bb := alloc(byte_string,112,0);
for k:=0 to 895 do;
if y mod 2=1 then mem_bset(bb,k) end;
y:=y**2 mod N;
end;
return string(mem_xor(bb,CCs));
end.
```

zu

```
Wurzelziehen modulo einer zusammengesetzten Zahl N ist schwierig, wenn die
Primfaktoren von N nicht bekannt sind
```

aufgelöst werden.