Mathematisches Institut
der Universität München
Pascal Reisert

Wintersemester 2015/2016
Übungsblatt 9
16. Dezember 2015

Übungen zur Algorithmischen Zahlentheorie
Lösung

Aufgabe 35

a) Das Polynom $X^e - X$ hat genau dann eine Nullstelle r in $\mathbb{Z}/N$ wenn $r_1^e = r_1 \bmod p$ und $r_2^e = r_2 \bmod q$ für die entsprechenden Elemente von $\mathbb{Z}/p \times \mathbb{Z}/q$ gilt. Über dem Körper $\mathbb{Z}_p$ hat $X^e - X = X(X^{e-1} - 1)$ aber gerade die Nullstellen 0 und $X^{e-1} = 1$, also $1 + \gcd(e-1, p-1)$ Nullstellen.[1] Da $p-1, q-1$ und damit auch $(p-1)(q-1)$ gerade ist, muss e mit $ed = 1 \bmod (p-1)(q-1)$ ungerade sein, also $e-1$ gerade sein. Damit ist $\gcd(e-1, p-1), \gcd(e-1, q-1) \geqslant 2$ und

$$(1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1) \geqslant 9.$$

Bemerkung. Die folgenden zwei Beweise der Aussage, dass $X^{e-1} - 1$ in $\mathbb{Z}/p$ genau $\gcd(e-1, p-1)$ Nullstellen hat, wurden von *Ludwig Fürst* und *Theresa Ullmann* in der Zentralübung vorgeschlagen und/oder vorgerechnet:

(I) Sei $d = \gcd(e-1, p-1)$. Dann gilt $\gcd(X^{e-1} - 1, X^{p-1} - 1) = X^d - 1$ (vgl. Aufgabe 13). Insbesondere ist eine Nullstelle x von $X^{e-1} - 1$ mit $x^f - 1 = 0$, $f | e-1, p-1 \Rightarrow f | d$ bereits eine Nullstelle von $X^d - 1$ und alle Nullstellen von $X^d - 1$ liegen in $(\mathbb{Z}/p)^*$, da alle Nullstellen - „$1, \ldots, p-1$“ - von $X^{p-1} - 1$ in $(\mathbb{Z}/p)^*$ liegen. Da die formale Ableitung dX^{d-1} von $X^d - 1$ für $d > 1$ wegen $d \nmid p$ nicht verschwindet, hat $X^d - 1$ genau d verschiedene Nullstellen.

(II) Wie zuvor sehen wir, dass eine Nullstelle Ordnung $k | d = \gcd(e-1, p-1)$ haben muss. Die endliche zyklische Gruppe $(\mathbb{Z}/p)^* = \langle g \rangle$ hat genau eine Untergruppe der Ordnung d - dies ist der Kern $K = \langle g^{p-1/d} \rangle$ des Endomorphismus $x \mapsto x^d$. Es gibt genau $\varphi(k)$ Elemente der Ordnung k in $(\mathbb{Z}/p)^*$. D.h. wir erhalten $|K| = \sum_{k|d, k \geqslant 1} \varphi(k) = d$.[2]

Aufgabe 36

a) Man beachte $k \geqslant 1$ da $e, d > 1$. Es folgt zunächst

$$\frac{1 + k\varphi(N)}{N} < \frac{1 + k(N-1)}{N} = k + \frac{1-k}{N} \leqslant k$$

und damit

$$\left| \frac{e}{N} - \frac{k}{d} \right| = \frac{1}{d} \left| \frac{1 + k\varphi(N)}{N} - k \right| = \frac{1}{d} \left(k - \frac{1 + k\varphi(N)}{N} \right)$$

[1] Sei $\langle g \rangle = (\mathbb{Z}/p)^*$ und $x = g^k, 0 \leqslant k < p-1, x^{e-1} = 1 \Rightarrow g^{k(e-1)} = 1 \Rightarrow p-1 | k(e-1) \Rightarrow k = j \cdot \frac{p-1}{\gcd(e-1, p-1)} < p-1 \Rightarrow j \in \{0, \ldots, \gcd(e-1, p-1) - 1\}$.

[2] Für die Eulersche φ-Funktion gilt $\sum_{k|d} \varphi(k) = d$: Sei $M_d(k) = \{1 \leqslant j \leqslant d : \gcd(j, d) = k\}$ und damit $\{1, \ldots, d\} = \dot{\bigcup}_k M_d(k)$. Dann ist $\varphi(d) = |M_d(1)|$ und $|M_d(k)| = \varphi(d/k)$. Also gilt $d = |\{1, \ldots, d\}| = \left| \dot{\bigcup}_k M_d(k) \right| = \sum_{k|d, k \geqslant 1} \varphi(d/k) = \sum_{k|d, k \geqslant 1} \varphi(k)$.

Wir schätzen $\varphi(N)$ nach unten ab. Gegeben unserer Nebenbedingung $q < p < 2q$ liefert $p = 2q \Rightarrow 2q^2 = N \Rightarrow q = \sqrt{N/2}$ die untere Schranke[3]

$$\varphi(N) > (\sqrt{N/2} - 1)(\sqrt{2N} - 1) = N + 1 - 3\sqrt{N/2}.$$

Wir erhalten

$$\frac{1}{d}\left(k - \frac{1 + k\varphi(N)}{N}\right) < \frac{1}{d}\left(k - \frac{1 + k(N + 1 - 3\sqrt{N/2})}{N}\right) = \frac{1}{d}\left(\frac{3k}{\sqrt{2N}} - \frac{(1+k)}{N}\right) < \frac{3}{\sqrt{N}},$$

da $d = \frac{1+k\varphi(N)}{e} > \frac{k\varphi(N)}{e} > k$.

b) Es gilt

$$\frac{1}{2d^2} > \frac{1}{2(\sqrt[4]{N}/3)^2} = \frac{9}{2\sqrt{N}} = \frac{3}{\sqrt{N}} \cdot \frac{3}{2} > \frac{3}{\sqrt{N}} > \left|\frac{e}{N} - \frac{k}{d}\right|$$

und somit ist k/d ein Kettenbruch.

c) Wir erhalten

```
function cfrac_appr(A,B,dbound: integer): array[2];
var
u0,u1,v0,v1,x0,x1,q,r: integer;
begin
    (u0,v0) := (1,0);
    (u1,v1) := (0,1);
    (x1,x0) := (A,B);
    while x1 /= 0 do
        (q,r) := divide(x0,x1);
        (u1,u0) := (q*u1 + u0, u1);
        (v1,v0) := (q*v1 + v0, v1);
        (x1,x0) := (r,x1);
        if v1 > dbound then break; end;
        if floor((u1/v1-A/B)*(2*(dbound**2)) )  = 0 then
            return (u1,v1);
        end;
    end;
    return (0,0);
end;

==> cfrac_appr(e,N,2**250).
-:
(1_55391_67413_70527_82914_19343_90027_56573_28051_17261_92676_33134_46718,
1_88853_33701_63134_89175_04431_07318_92661_40042_86123_55649_53830_58897
```

Man verwende die Beziehung

$$ed = 1 + k(p-1)(q-1) = 1 + k(N + 1 - p - q) \Rightarrow p + q = (N+1) + \frac{1 - ed}{k}.$$

[3] $N - q - N/q + 1 \xrightarrow{\partial_q} -1 + N/q^2 < 0$ fällt monoton für $q < \sqrt{N}$. Wähle q minimal mit $qp = N, p < 2q$.

p+q=
23146_91887_17176_89788_44681_24851_38268_13029_91622_78977_71436_44224_
96224_10789_87674_49624_04951_22775_10723_69851_20558_82125_81893_38784_
73371_07413_64116_92289_78455_45234_34978

Jetzt kann die quadratische Gleichung $X^2 - (p+q)X + pq = 0$ wie üblich gelöst werden. Wir erhalten die Diskriminante

7620_14710_19795_59319_63732_95745_39945_32295_61150_60813_63357_47580_
16273_37046_80909_65916_55831_52655_32417_53264_48589_87036_42182_45147_
73427_51086_09452_77156_45525_36201_28804

und damit

q=
7763_38588_48690_65234_40474_14552_99161_40367_15236_09082_04039_48322_
39975_36871_53382_41853_74559_85059_89153_08293_35984_47544_69855_46818_
49971_78163_77332_07566_66465_04516_53087

p=
15383_53298_68486_24554_04207_10298_39106_72662_76386_69895_67396_95902_
56248_73918_34292_07770_30391_37715_21570_61557_84574_34581_12037_91966_
23399_29249_86784_84723_11990_40717_81891.