Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 5
14. November 2018

Übungen zur Kryptographie
Lösung

Aufgabe 18

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.[2] Damit ist $\gcd(e-1, p-1), \gcd(e-1, q-1) \geq 2$ und

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

b) Sei x unser nicht-trivaler Fixpunkt. Angenommen $\gcd(x, N) \neq 1$, dann sind wir fertig. Sei nun x invertierbar, dann hat x Ordnung $o | e-1$ in $\mathbb{Z}/N$. Für das Bild[3] (x_1, x_2) in $\mathbb{Z}/p \times \mathbb{Z}/q$ gilt entsprechend $x_1^o = 1$, $x_2^o = 1$, also gibt es o', o'' mit $o' | \gcd(e-1, p-1) = 2$ und $o' | \gcd(e-1, q-1) = 2$. Wegen der Nichttrivialität wissen wir bereits o.B.d.A. $o' = 1$, $o'' = 2$ und $o = 2$. Angenommen $x \pm 1$ ist ebenfalls invertierbar, so gilt

$$(x \pm 1)^2 = (\pm 2x + 2) = 2(\pm x + 1) \Rightarrow x \pm 1 = \pm 2 \Rightarrow x = \pm 1$$

im Widerspruch zur Nichttrivialität von x. Somit sind $\gcd(x \pm 1, N)$ die nicht-trivialen Teiler p, q von N.

Bemerkung. Ist $\gcd(x, N) \neq 1$, dann ist entweder $x+1$ oder $x-1$ ein nicht-invertierbarer Fixpunkt, da das Bild in $\mathbb{Z}/p \times \mathbb{Z}/q$ entweder $(1,0), (0,1), (-1,0)$ oder $(0,-1)$ ist. Somit haben wir die beiden Teiler $\gcd(x, N)$, $\gcd(x+1, N)$ oder $\gcd(x, N)$, $\gcd(x-1, N)$ von N gefunden. Ist $x \pm 1$ nicht-invertierbarer Fixpunkt, so kann $x \mp 1$ nur invertierbar sein, da $p, q > 2$ nicht gleichzeitig $x+1$ und $x-1$ teilen können.
Die drei Werte $\gcd(x-1, N)$, $\gcd(x, N)$, $\gcd(x+1, N)$ liefern also immer p, q.

c) Es ist $47383481 = 6571 \cdot 7211$ und $\gcd(6570, 32) = \gcd(7210, 32) = 2$. Es gibt also 9 Fixpunkte.
Man beachte, dass $1476 \cdot 6571 - 1345 \cdot 7211 = 1$, sowie $0, 1, -1$ Nullstellen von $X^e - X = 0$ in $\mathbb{Z}/p$ sind. Letzteres folgt, da $(-1)^e = -1$, da e ungerade ist. Wir erhalten somit unter $\mathbb{Z}/p \times \mathbb{Z}/q \to \mathbb{Z}/N$

$$(0,0) \mapsto 0 \bmod N,\ (1,1) \mapsto 1 \bmod N,\ (-1,-1) \mapsto -1 \bmod N,$$

$$(0,1) \mapsto -1345 \cdot 7211 = 37684686 \bmod N,\ (1,0) \mapsto 1476 \cdot 6571 = 9698796 \bmod N,$$

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

[2] Man beachte, dass es genügt, dass der größte gemeinsame Teiler ungerade ist.

[3] $x_1 \neq 0 \neq x_2$.

$$(0,-1) \mapsto 1345 \cdot 7211 = 9698795 \bmod N,\ (-1,0) \mapsto -1476 \cdot 6571 = 37684685 \bmod N,$$
$$(-1,1) \mapsto -1476 \cdot 6571 - 1345 \cdot 7211 = 27985890 \bmod N,$$
$$(1,-1) \mapsto 1476 \cdot 6571 + 1345 \cdot 7211 = 19397591 \bmod N,$$

Die gesuchten Fixpunkte sind

$$0, 1, 9698795, 9698796, 19397591, 27985890, 37684685, 37684686, 47383480.$$

Bemerkung. Zwei weitere Beweise der Aussage, dass $X^{e-1} - 1$ in $\mathbb{Z}/p$ genau $\gcd(e-1, p-1)$ Nullstellen hat:

(I) Sei $d = \gcd(e-1, p-1)$. Dann gilt $\gcd(X^{e-1} - 1, X^{p-1} - 1) = X^d - 1$. 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 $|K| = \sum_{k|d, k \geq 1} \varphi(k) = d$.[4]

Da 33 nicht invertierbar ist, kann man z.B. $e = 37$ verwenden, um ein RSA-System zu erhalten. In diesem Fall ist $37 \cdot 7681573 - 6 \cdot 47369700 = 1$. Wir erhalten die 57 Fixpunkte

$$0, 1, 57689, 1463833, 1478255, 1514309, 1514310, 2942088, 3230529, 6410578, 6468267,$$
$$6756708, 8184486, 8220541, 8234963, 9641107, 9698795, 9698796, 11162629, 11177051,$$
$$11213105, 11213106, 12640884, 16109374, 16167063, 19339903, 19397591, 20911901,$$
$$21575311, 25808170, 26471580, 27985890, 28043578, 31216418, 31274107, 34742597,$$
$$36170375, 36170376, 36206430, 36220852, 37684685, 37684686, 37742374, 39148518,$$
$$39162940, 39198995, 40626773, 40915214, 40972903, 44152952, 44441393, 45869171,$$
$$45869172, 45905226, 45919648, 47325792, 47383480.$$

Da sowohl $X^2 - 1$ als auch $X^4 - 1$ genau die beiden Nullstellen ± 1 haben, ergeben sich die weiteren Nullstellen von $X^{36} - 1 \bmod 6571$ aus einer primitiven 9ten Einheitswurzel g modulo 6571 als $g^k, -g^k, k = 0, \ldots, 8$. Ein Beispiel ist $g = -220$. Anschließend kann man wieder zusammensetzen, z.B. $(g, 1) \in \mathbb{Z}/6571 \times \mathbb{Z}/7211$ entspricht $220 \cdot 1345 \cdot 7211 + 1476 \cdot 6571 = 11177051$.

Aufgabe 19

a) Es gilt $ed \equiv 1 \bmod \varphi(N)$ für eine Zahl d und $(x^e \bmod N)^d = x^{ed} \bmod N = x \bmod N$, da $(x^e + kN)^d = x^{de} + N \sum_{j=0}^{d-1} \binom{d}{j} x^{je} (kN)^{d-j-1} \equiv x^{de}$. Da $e \in (\mathbb{Z}/\varphi(N))^\times$ existiert ein $k = \mathrm{ord}(e)$ mit $e^k = 1 \bmod \varphi(N)$. Somit gilt mit $m = k-1$: $1 = e^k = e \cdot e^m = ed \Rightarrow e^m = d$ und folglich $E^m(E(x)) = (x^e)^{e^m} = x^{e^k} = x \bmod N$.

[4] Für die Eulersche φ-Funktion gilt $\sum_{k|d} \varphi(k) = d$: Sei $M_d(k) = \{1 \leq j \leq d : \gcd(j, d) = k\}$ 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 $d = |\{1, \ldots, d\}| = \left|\dot{\bigcup}_k M_d(k)\right| = \sum_{k|d, k \geq 1} \varphi(d/k) = \sum_{k|d, k \geq 1} \varphi(k)$.

b) Im ersten Fall ist $\varphi(55) = 4 \cdot 10 = 40$ und $d = 27 = 3^3, m = 3$. Wir wir bereits in Aufgabe 18 festgestellt haben ist 33 nicht invertierbar in $\mathbb{Z}/47369700$. Für 37 ergibt sich z.B. $47383481 = 6571 \cdot 7211$, also $\varphi(47383481) = 6570 \cdot 7210 = 47369700$ und $d = 7681573, m = 3059$. Alternativ kann man wie in Aufgabe 17 die Ordnung von 37 modulo $\mathrm{lcm}(6570, 7210)$ berechnen und erhält damit $m = 611$.

Aufgabe 20

Wir berechnen wieder zuerst $62663 = 223 \cdot 281$ und damit $\varphi(62663) = 62160$ und $17 \cdot 7313 \equiv 1 \bmod 62160$. Weiter ist z.B. `B186` $\equiv 177 \cdot 256 + 134 = 45446$ und $45446^{7313} \equiv 21097 = 82 \cdot 256 + 105 \equiv$ `5269`.
In Aribas kann dies wie folgt umgesetzt werden:

```
function cry(N,e:integer; K:byte_string):byte_string;
var
u,v,a,b,k,l: integer;
C:byte_string[length(K)];
begin
l:=length(K) div 2;
for k:=0 to l-1 do
u:=K[2*k]*256+K[2*k+1];
v:=u**e mod N;
a:=v div 256;
b:=v mod 256;
C[2*k]:=a;
C[2*k+1]:=b;
end;
return C;
end;
K:=$B186_E9E9_EF9D_3AD9_44F9_21D4_5B5F_E46B_463E_6FD1_D3DF;
cry(62663,7313,K);
string(_).
```

Es ergibt sich:

```
-: "Rivest/Shamir/Adleman "
```