Prof. Dr. Gregor Leander
WS 2016/17

Thorsten Kranz
Friedrich Wiemer

Hausaufgabe 2

Aufgabe 2.1

Schreibe die folgende Funktion, die mittels Baby-Step/Giant-Step Algorithmus den diskreten Logarithmus von a zur Basis g löst. a ist dabei ein beliebiges Element aus einer zyklischen Gruppe $\langle g \rangle$ mit Gruppenoperation $\circ =$ op. Der BSGS Algorithmus muss von euch selbst implementiert werden.

```
def my_bsgs(a, g, op):
    """
    Implementierung des Baby-Step/Giant-Step Algorithmus
    Eingabe: a, g, mit a = g^b
    Ausgabe: b
    """
    pass
```

Aufgabe 2.2

Nutze `my_bsgs` als Unterroutine in der der folgenden Funkion, die den Silver-Pohlig-Hellman Algorithmus implementiert. Der SPH Algorithmus muss von euch selbst implementiert werden. Für den Chinesischen Restsatz könnt ihr die `crt` Sage Funktion verwenden, zur Faktorisierung der Gruppenordnung die `factor` Sage Funktion.

```
def my_sph(a, g, op):
    """
    Implementierung des Silver-Pohlig-Hellman Algorithmus
    Eingabe: a, g, mit a = g^b
    Ausgabe: b
    """
    pass
```

Tipps:

```
crt?                        # Sage Hilfe: crt Funktion mit Beispiel
op = lambda x,y: x * y      # Definition der Gruppenoperation
g = Integers(41)(3)         # Beispiel Aufruf der Funktionen
a = g^2
b = my_bsgs(a, g, op)
a == g^b
b = my_sph(a, g, op)
a == g^b
a == op(g, g)
```

Aufgabe 2.3

Berechnet für folgende Werte mit eurer Implementierung $\mathrm{dlog}_g(a)$.

1.
   - Gruppe: $(\mathbb{Z}_n, +)$ mit $n = 1459 \cdot 1531 = 2233729$
   - $a = 1229675$
   - $g = 1$
2.
   - Gruppe: $(\mathbb{Z}_p^*, \cdot)$ mit $p = 1048368573847272683495828220422329672575844726363$
   - $a = 217453653188290399527611156904936031780712799 06$
   - $g = 5$
3.
   - Gruppe: $(\mathbb{Z}_p^*, \cdot)$ mit $q = 1328285643735126382990952801509744620675700621313$
   - $a = 1220545409488630044674899266837356079889084495432$
   - $g = 5$
4.
   - Gruppe: elliptische Kurve $\mathcal{E}$ definiert durch $y^2 = x^3 + u \cdot x + v \bmod q$, mit den Parametern
     - $u = 561849381776711487400135240742334441879816575281$
     - $v = 1224742114973299634178166497109881746220902530269$
     - $q = 1328285643735126382990952801509744620675700621313$

     und der bekannten Gruppenoperation auf der Kurve.
   - $a = (x_a : y_a : 1)$
     $x_a = 1055992796642808793006780521119047311544165188440$
     $y_a = 565550177502760842377259480613952441780797553104$
   - $g = (x_g : y_g : 1)$
     $x_g = 605422826550677733905661001980627216893075411015$
     $y_g = 860376159671298479041797365702737250175014167 10$