Hochschule Bonn-Rhein-Sieg

Angewandte Kryptographie 2, SoSe 2024

Vorlesungsteil "Kryptographie mit elliptischen Kurven"
Guntram Wicke (guntram.wicke@lehrbeauftragte.h-brs.de)

# 1 Übungen zu Kapitel 1 ("Preliminaries")

## 1.1 Größter gemeinsamer Teiler (ggT), engl. "greatest common divisor" (gcd)

Berechnen Sie den größten gemeinsamen Teiler $d$ von $x$ und $y$ sowie die Koeffizienten $a$ und $b$ der folgenden Linearkombinationen $ax+by = d$ mit $a, b, d, x, y \in \mathbb{Z}$. Wie viele Iterationen braucht der Erweiterte Euklidische Algorithmus jeweils?

1. $x = 126, y = 35$.
2. $x = 89, y = 55$.
3. (sage/python)
   $x = 768849563970453442208097466290016490930379502009430552037356014450315161977 51$,
   $y = 591060745269802798160910548559906496989105405741052699797531713650050469197 80$.

## 1.2 Kongruenzen, additive und multiplikative Inverse in $(\mathbb{Z}/n\mathbb{Z})$

Stellen Sie fest, ob die Elemente $a$ und $b$ aus $(\mathbb{Z}/n\mathbb{Z})$ zueinander kongruent sind.

1. n=60, a=133, b=45
2. n=60, a=133, b=613
3. (sage/python)
   $n = 768849563970453442208097466290016490930379502009430552037356014450315161977 51$,
   $a = 591060745269802798160910548559906496989105405741052699797531713650050469197 80$,
   $b = 121238042048266044312823725429101538609447979358825109803578719304047778988 6045$.

Geben Sie additive und multiplikative Inverse zu $a$ aus $(\mathbb{Z}/n\mathbb{Z})$ an, falls sie existieren:

1. $n = 126$, $a = 35$.
2. $n = 89$, $a = 55$.
3. (sage/python)
   $n = 768849563970453442208097466290016490930379502009430552037356014450315161977 51$,
   $a = 591060745269802798160910548559906496989105405741052699797531713650050469197 80$.