Einschub

Was ist mit ?

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **\*** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
| **0** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| **2** | 0 | 2 | 4 | 6 | 8 | 10 | 0 | 2 | 4 | 6 | 8 | 10 |
| **3** | 0 | 3 | 6 | 9 | 0 | 3 | 6 | 9 | 0 | 3 | 6 | 9 |
| **4** | 0 | 4 | 8 | 0 | 4 | 8 | 0 | 4 | 8 | 0 | 4 | 8 |
| **5** | 0 | 5 | 10 | 3 | 8 | 1 | 6 | 11 | 4 | 9 | 2 | 7 |
| **6** | 0 | 6 | 0 | 6 | 0 | 6 | 0 | 6 | 0 | 6 | 0 | 6 |
| **7** | 0 | 7 | 2 | 9 | 4 | 11 | 6 | 1 | 8 | 3 | 10 | 5 |
| **8** | 0 | 8 | 4 | 0 | 8 | 4 | 0 | 8 | 4 | 0 | 8 | 4 |
| **9** | 0 | 9 | 6 | 3 | 0 | 9 | 6 | 3 | 0 | 9 | 6 | 3 |
| **10** | 0 | 10 | 8 | 6 | 4 | 2 | 0 | 10 | 8 | 6 | 4 | 2 |
| **11** | 0 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Welche Elemente sind invertierbar?

(„“)  
 („“)  
   
Welche Elemente sind nicht invertierbar?

Z.B.: ist nicht invertierbar, weil …  
… es ein Nullteiler ist ()  
… nicht lösbar ist  
… nicht in der steht  
… ich weiß nicht ob oder ist  
… 4 und 12 sind nicht teilerfremd

Wenn m keine Primzahl ist:

* Hat Nullteiler
* Ist kein Körper
* Es gibt nicht invertierbare Elemente
* Dividieren ist nicht durch alle Elemente möglich

Verschlüsseln geht so nicht, weil und (\*). Entschlüssler weiß nicht, ob oder Klartext ist.

Wenn m Primzahl ist:

* ist ein Körper

Verschlüsselung“ 6.8: , Schlüssel

Klartext:

Chiffretext:

Entschlüsseln durch „Dividieren“ = Multiplizieren mit dem Inversen

Antwort:

Probe:

Um zu einer Zahl a in das multiplikative Inverse zu finden, kann man den erweiterten euklidischer Algorithmus verwenden.

Wir berechnen den ggT von 735 und 2079

1. Primfaktorzerlegung  
      
      
    logisch, aber für große Zahlen sehr aufwendig
2. Alternative: Euklidischer Algorithmus  
   Man subtrahiert immer wieder die kleinere von der größeren Zahl. Die letzte Zahl (vor null) ist der ggT.  
    =   
    =   
    =   
    =   
    =   
    =   
    =   
    =   
    =   
    =   
    =   
    =   
    =   
   => 2079 und 735 sind nicht teilerfremd, sie haben ggT 21  
   => in nicht invertierbar
3. Erweiterter euklidischer Algorithmus  
   Es ist immer möglich, auf folgende Art den ggT zu berechnen.  
   Wir suchen

Was nützt uns das?

,

~

|  |  |  |
| --- | --- | --- |
|  | s | t |
| 26 | 1 | 0 |
| 5 | 0 | 1 |
| 21 | 1 | -1 |
| 16 | 1 | -2 |
| 11 | 1 | -3 |
| 6 | 1 | -4 |
| 1 | 1 | -5 |
| 4 | -1 | 6 |
| 3 | -2 | 11 |
| 2 | -3 | 16 |
| 1 | -4 | 21 |
| 0 | 5 | -26 |

Alles in , also sind 26 und 5, teilerfremd

In : ist invertierbar, sein Inverses ist

In : das Inverse von siehe Bsp. 6.8.

|  |  |  |
| --- | --- | --- |
| 153 | 1 | 0 |
| 82 | 0 | 1 |
| 71 | 1 | -1 |
| 11 | -1 | 2 |
| 5 | 7 | -13 |
| 1 | -15 | 28 |
| 1 | 7+(-15)\*(-4) = | -13+28\*(-4)= |
| 0 |  |  |

=> sind teilerfremd

ist invertierbar

ist invertierbar  
 Ist Inv.

Rechenbeispiel:

|  |  |  |
| --- | --- | --- |
| 318 | 1 | 0 |
| 186 | 0 | 1 |
| 132 | 1 | -1 |
| 54 | -1 | 2 |
| 24 | 3 | -5 |
| 6 | -7 | 12 |
| 0 | … | … |

=> nicht invertierbar  
 nicht lösbar

=> nicht invertierbar

Nach Addieren und Multiplizieren und Untersuchen der Umkehroperationen (zu +: immer möglich und einfach, zu \*: nur möglich wenn teilerfremd zu Modul, und (für Computer) einfach über EEA beschäftigen wir uns mit Potenzieren.

wir bewegen uns in : Dann kann man mit folgende Potenzen bilden:

Dabei kann nie vorkommen, weil p Primzahl ist. Nach spätestens -Schritten wiederholt sich alles, weil nur Elemente hat.

Gegenbeispiel: ,

Echtes Beispiel:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Lässt sich Potenzieren umkehren?

Gibt es eine Lösung für Folgendes:

hier Ja, wenn oder , dann kann beliebig sein. Mit , wenn . Mit nur, wenn

X heißt dann, diskreter Logarithmus von b zur Basis a

Wie berechnet man den diskreten Logarithmus?

Durch Ausprobieren! (es gibt kaum effizientere Algorithmen)