Primzahlen

Ritter, Wende, Zehentbauer

Gliederung

- Definition
- Fun facts und besondere Primzahlen
- Primzahl-Algorithmen
  - Brute Force
  - Sieb des Eratosthenes
  - Fermatscher Primzahltest
  - Miller Rabin Test
- Golbachsche Vermutung
- Primfaktorzerlegung
- RSA Kryptosystem

Definition

Eine natürliche Zahl n > 0 heißt Primzahl, wenn 1 und n ihre einzigen positiven Teiler sind.

z.B.: 2,3,5,7,11,13,17,19,23,29....

Eine Primzahl ist also eine Zahl mit genau 2 Teilern, daher zählt die 1 nicht zu den Primzahlen, da sie nur einen Teiler besitzt!

Zusammengesetzte Zahlen

Natürliche Zahlen die KEINE Primzahlen sind, werden als zusammengesetzte Zahlen bezeichnet.

Jede zusammengesetzte Zahl lässt sich durch Multiplikation von Primzahlen darstellen (Primfaktorzerlegung).

Man könnte also sagen, dass Primzahlen die Atome der natürlichen Zahlen sind.

Eine Außnahme bildet hierbei die Zahl 1.

Euklids Beweis

Beginnend mit der Annahme einer endlichen Menge an Primzahlen stellen wir die Gleichung

$N = p_1 \times p_2 \times p_3 \times \ldots \times p_r + 1$ mit p_r als größte Primzahl auf.

Diese generierte Zahl lässt sich durch keine der in unserer Menge vorhandenen Primzahlen Teilen da $N\%p_i = 1$.

Folglich ist die Anfängliche Annahme widerlegt und es kann von unendlich vielen Primzahlen ausgegangen werden.

Fun facts

Preisgelder für die Entdeckung neuer Primzahlen:

Primzahl mit 100 Millionen Stellen = 150.000 $

Primzahl mit einer Milliarde Stellen = 250.000 $

Die größte bekannte Primzahl hat 12978189 Stellen. Es ist die Zahl 2^43112609 – 1.

Sie wurde 2008 entdeckt, als erste Primzahl mit über 10 Millionen Ziffern.

Besonderheiten

Jede Primzahl > 3 lässt sich durch 6n-1 oder 6n+1 darstellen.

z.B. 37 = 6*6+1

Zwei natürliche Zahlen deren Summe eine Primzahl ergibt, sind immer teilerfremd.

z.B. 8 + 9 = 17

Viellinge

Ein Primzahlzwilling ist ein Paar aus Primzahlen, deren Abstand 2 ist. zB: 3/5, 5/7, 11/13...

Ein Primzahldrilling ist eine Menge aus Primzahlen der Form p,p+2,p+6 oder p,p+4,p+6.

z.B.: 5/7/11, 7/11/13, 13/17/19...

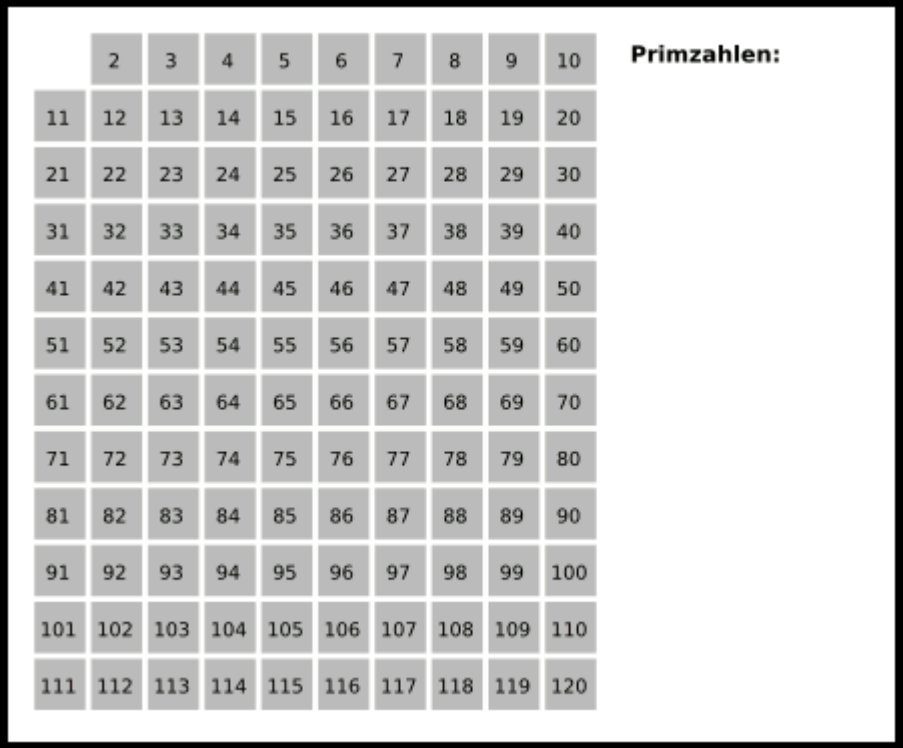
Ein Primzahlvierling besteht aus zwei Primzahlzwillingspaaren im Abstand 4. zB: 5/7/11/13, 11/13/17/19, 191/193/197/199...

Brute Force

```
        if(number <= 1)
                return false;
        for(int i = 2; i < number; i++){
                if(number%i == 0)
                        return false;
        }
        return true;
}
```

Sieb des Eratosthenes

Sieb des Eratosthenes



Fermatscher Primzahltest

$a^{p-1} \equiv 1 \bmod p$

➔ $a^{(p-1)} \bmod p = 1$

➔ ist mögliche Primzahl

Achtung vor Pseudoprimzahlen

(Carmichael-Zahl z.B. 561)!

Miller-Rabin-Test

p = ungerade

$p - 1 = u * 2^i$

GGT(u, p) = 1

$y_0 = a^{(u * 2i)} \bmod p = p - 1$

Wahrscheinlichkeit für Primzahl $> 1 - (1/4)^t$

Mersennesche Primzahlen

$$M_n = 2^n - 1$$

$n = \{2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127\}$

Durch $n = a*b$ kann M_n nicht prim sein und somit lassen sich zerlegbare Zahlen ausschließen.

Goldbachs Vermutung

Jede gerade Zahl > 2 lässt sich als Summe zweier Primzahlen darstellen.

Ist bis heute unbewiesen.

Bis zur Zahl 100.000.000 ist die Vermutung allerdings erprobt

Primfaktorzerlegung

Jede Zahl lässt sich in ihre Primfaktoren zerlegen, z.B. 44 = 2, 2, 11.

Mit den Primfaktoren lässt sich die Anzahl der Teiler ermitteln: $a^x + b^y + c^z$...

anzahlTeiler = (x+1)*(y+1)*(z+1).

z.B. 44 = $2^2 + 11^1$ -> anzahlTeiler = 6

(1, 2, 4, 11, 22, 44)

RSA Kryptosystem

Wähle 2 möglichst große Primzahlen p und q (p!=q)

Rechne N für N = p*q aus

Berechne $Phi_{(N)}$ für $Phi_{(N)} = (p-1)*(q-1)$

Wähle eine Zahl e die Teilerfremd zu $Phi_{(N)}$ ist ($e<Phi_{(N)}$)

Berechne aus e das modular inverse d (erweiterter Euklidscher Algorithmus) zu N

($e*d \equiv 1 \bmod Phi_{(N)}$)

e wird Primary Key und d als Public Key bezeichnet

RSA Kryptosystem

p,q und $Phi_{(N)}$ werden nicht mehr benötigt (Löschen!)

Der zu verschlüsselnde Text als Zahl K wird verschlüsselt mit:
$C \equiv K^e \bmod N$ (umgestellt: $K^e \bmod N = C$)

Der verschlüsselte Text C wird entschlüsselt mit:
$K \equiv C^d \bmod N$ (umgestellt: $C^d \bmod N = K$)

Quellenangabe

Algorithmen und Problemlösungen mit C++ Doina Logofatu

http://www.wikipedia.org

http://www.mathe-online.at

☺ Vielen Dank für Ihre Aufmerksamkeit ☺