Sieb des Eratosthenes

Suchen alle Primzahlen bis zu einer Zahl $n \in \mathbb{N}$. Dann: $n = 36$ $\sqrt{n} = 6$

~~1~~ (2) (3) ~~4~~ (5) ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11
~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ 21
~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31
~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~

Hier sei entsteht eine weitere Idee:

$P := \prod_{i \in I} p_i$ p_i Primzahlen

$ggT(P, N) \neq 1$, so haben wir Teiler unter den p_i

$= 1$, so wissen wir, dass keines der p_i N teilt

Man sollte sich eine Strategie ausdenken für beliebige N.

Fermats Idee

Sei $N \in \mathbb{N}$ ungerade und eine zusammengesetzte Zahl, also

$N = a \cdot b$ $\quad a, b \in \mathbb{N}$ ungerade

Durch die Wahl von $x, y \in \mathbb{N}$ mit

$$x := \frac{a+b}{2} \quad \text{und} \quad y := \frac{a-b}{2}$$

können wir auch schreiben:

$$N = (x+y)(x-y) = x^2 - y^2$$

Wir suchen also ein Quadrat, das die folgende Gleichung erfüllt:

$$y^2 = x^2 - N$$

Dazu beschreib Fermat folgenden Algorithmus:

$x := \lfloor \sqrt{N} \rfloor + 1$ $\quad$ fortfahren: $= x^2 - N$

Erweiterung der Idee

(durch Gauß (1777-1855), Legendre (1752-1833) und später in den 20er Jahren Kraitchik (1882-1957))

Sie fanden heraus, das man auch folgendes suchen kann:

$$x^2 - y^2 = (x+y)(x-y) = kN \qquad k \in \mathbb{N}$$

Daraus folgt, dass in dem Restklassenring $\mathbb{Z}/N\mathbb{Z}$ für x^2 die Wurzel y ex.

Wir suchen also:

$$x^2 \equiv_N y^2 \quad \text{mit} \quad x \not\equiv_N \pm y$$

Finden wir ein solches y, so können wir über den

$$ggT(x-y, N)$$

einen nicht-trivialen Teiler von N finden.

Allg. Vorgehensweis bei den im Folgenden beschriebenen Algorithmen:

Wir bestimmen quadratische Reste

$z_i \equiv_N x_i^2 \qquad z_i \in \mathbb{Z} \qquad i \in S := \{1 \dots s\}$

und versuchen durch geschickte Wahl von $I \subseteq S$ folgendes zu finden:

$\prod_{i \in I} z_i = y^2$ ein Quadrat in $\mathbb{Z}$,

wähle dann: $x := \prod_{i \in I} x_i$

$$\Rightarrow x^2 \equiv_N y^2$$

$y^2 \equiv_N x^2$ mit $x \not\equiv_N \pm y$

Es gibt genau 2^d verschiedene Wurzeln von x^2 ($d \triangleq$ Anzahl Primteiler von N)

Zur Ex. von solchen y:

sei dazu N ungrade, keine Primzahl

Sei $N = a \cdot b$ a, b teilerfremd

$y \in \mathbb{Z}_N^*$

$\overset{CRS}{\Rightarrow}$ $\exists\, x \in \mathbb{Z}_N^*$ mit $\underbrace{x \equiv_a y}_{*}$ $x \equiv_b -y$

d.h. $a \mid x-y$ und $b \mid x+y$

also: $x^2 \equiv_N y^2$

Es bleibt zu zeigen, $x \not\equiv \pm y$

Nehmen das Gegenteil an $x \equiv_N +y$ oder $x \equiv_N -y$

OE $x \equiv_N -y$

$\Rightarrow$ $x \equiv_a -y$ aber auch $x \equiv_a y$ (*)

$\Rightarrow$ $2x \equiv_a 0$ da a ungerade $\Rightarrow a \mid x$

$\Rightarrow$ $ggT(x, N) \neq 1$ ↯ $x \in \mathbb{Z}_N^*$

Dazu müssen wir uns Folgendes vorstellen:

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus_i \dots \oplus_i \mathbb{Z}/p_d^{e_d}\mathbb{Z}$$

$$z = (z_1, \dots, z_d)$$

$$\| \quad (y_1^2, \dots, y_d^2) = y^2$$

<u>Wurzeln</u> von $(z_1, \dots, z_n)$ sind demnach $(\pm y_1, \dots, \pm y_d)$

Warum gibt es (genau) 2^d Stück, obwohl wir uns in Ringen befinden?

Dazu: Es existieren keine oder zwei Quadratwurzeln einer Zahl $a \in \mathbb{Z}/p^e\mathbb{Z}^*$ $a \neq 0$ $p \neq 2$

Seien $x, y \in \mathbb{Z}/p^e\mathbb{Z}$ Quadratwurzel von a

Dann ist $x^2 - y^2 = k p^e \quad k \in \mathbb{Z}$

also $(x+y)(x-y) = k p^e$ (*)

Es kann aber nicht sein, dass $x+y$ und $x-y$ durch p^e teilbar sind, dann würde folgen

$y \equiv_{p^e} -y \Rightarrow y = 0 \Rightarrow a = y^2 = 0$ ↯ (*)

Also ist entweder $x+y$ oder $x-y$ teilbar durch p^e (nach *)

$\Rightarrow x = y$ oder $x = -y$

Das Quadratische Sieb

Vorgegeben: $N \in \mathbb{N}$ zusammengesetzt, keine Primzahlpotenz.

Parameter $B, S \in \mathbb{N}$

Gesucht: $X^2 \equiv_N Y^2$

1. Liste: $L = [f_1, \dots, f_S]$.

$f_i := f(x_i) := x_i^2 - N, \quad x_i := \lfloor \sqrt{N} \rfloor + i$

2. Faktorbasis: $F(B) := \{ p \le B \mid p \text{ prim}, \left(\frac{N}{p}\right) = 1 \}$

3. Sieben: - Suche für $p \in F(B)$ Lösung t von $x^2 \equiv_p N$

- setze $t_1 := t - \lfloor \sqrt{N} \rfloor \bmod p$,
  $(p \neq 2)$ $t_2 := -t - \lfloor \sqrt{N} \rfloor \bmod p$
- dann $L[t_j + k \cdot p] = f_{t_j + kp}$, $j = 1,2$, $k \in \mathbb{N}$
  durch p teilen
- für p^e, $e \ge 2$ evtl. wiederholen

4. Y^2 ermitteln: - für $L[i] = 1$ Faktorbasisvektoren erzeugen
- Lin. Abh. der Vektoren mod 2 suchen
- sein $(v(f_{i_1}), \dots, v(f_{i_e}))$ l. a.
  $\Rightarrow Y^2 := \sqrt{f_{i_1} \cdot \dots \cdot f_{i_e}} \bmod N$

5. Auswertung: $X := x_{i_1} \cdot \dots \cdot x_{i_e} \bmod N$, $ggT(X - Y, N)$ berechnen

Das Quadratische Sieb

Vorgegeben: $N \in \mathbb{N}$ zusammengesetzt, keine Primzahlpotenz.

Parameter $B, S \in \mathbb{N}$

Gesucht: $X^2 \equiv_N Y^2$

1. Liste: $L = [f_1, \dots, f_S]$.

$f_i := f(x_i) := x_i^2 - N, \quad x_i := \lfloor \sqrt{N} \rfloor + i$

2. Faktorbasis: $F(B) := \{ p \le B \mid p \text{ prim}, \left(\frac{N}{p}\right) = 1 \}$

3. Sieben: - Suche für $p \in F(B)$ Lösung t von $x^2 \equiv_p N$

- setze $t_1 := t - \lfloor \sqrt{N} \rfloor \bmod p$,
  $(p \neq 2)$ $t_2 := -t - \lfloor \sqrt{N} \rfloor \bmod p$
- dann $L[t_j + k \cdot p] = f_{t_j + kp}$, $j = 1, 2$, $k \in \mathbb{N}$
  durch p teilen
- für p^e, $e \ge 2$ evtl. wiederholen

4. Y^2 ermitteln: - für $L[i] = 1$ Faktorbasisvektoren erzeugen
- Lin. Abh. der Vektoren mod 2 suchen
- sein $(v(f_{i_1}), \dots, v(f_{i_\ell}))$ l. a.
  $\Rightarrow Y^2 := \sqrt{f_{i_1} \cdot \dots \cdot f_{i_\ell}} \bmod N$

5. Auswertung: $X := x_{i_1} \cdot \dots \cdot x_{i_\ell} \bmod N$, $ggT(X - Y, N)$ berechnen

4. Quadrat Y^2 ermitteln

Seien $f_{i_1}, \ldots, f_{i_r}$ B-glatt,

also $f_{ij} = p_1^{e_{1j}} \cdot \ldots \cdot p_b^{e_{bj}}$ $b = |F(B)|$,
$j = 1, \ldots, r$

$$V(f_{ij}) := (e_{1j}, \ldots, e_{bj})^{tr}$$

„Faktorbasisvektor"

$$M := \left(V(f_{i_1}) \cdots V(f_{i_r}) \right) = \begin{pmatrix} e_{11} & \cdots & e_{r1} \\ \vdots & \ddots & \vdots \\ e_{b1} & \cdots & e_{br} \end{pmatrix} \in \mathbb{N}_0^{b \times r}$$

$\rightarrow$ $\ker(M \bmod 2)$ berechnen

für $V^{\oplus}$ setzte:

$$V(\widetilde{Y}) := \frac{1}{2}(M \cdot v) \rightsquigarrow \widetilde{Y} \equiv_N Y \in \{0, \ldots, N-1\}$$

Σ: ~~$\widetilde{X} := (x_{i_1}, \ldots, x_{i_r})\, v$~~ $\rightsquigarrow \widetilde{X} \equiv_N X \in \{0, \ldots, N-1\}$

$X \equiv_N \pm Y$ überprüfen

$\Rightarrow$ $ggT(X+Y, N)$ / $ggT(X-Y, N)$

ist dann nicht-trivialer Teiler von N

Beispiel:

$N = 2041, \lfloor \sqrt{N} \rfloor = 45, \quad B = 10,5 - 8$

x_i	46	47	48	49	50	51	52	53
$f_i = x_i^2 - N$	75	168	263	360	459	560	663	768

$L = [75, 168, 263, 360, 459, 560, 663, 768]$

$F(10) = \{2, 3, 5, 7\}$

$p=2: L = [75, 21, 263, 45, 459, 35, 663, 3]$

$p=3: \quad N \equiv_3 1 \equiv_3 1^2 \equiv_3 2^2$

1. $1 \equiv_3 46 \quad L = [25, 21, 263, 15, 459, 35, 221, 3]$
2. $2 \equiv_3 47 \quad L = [25, 7, 263, 15, 153, 35, 221, 1]$

$g: \quad N \equiv_g 7 \equiv_g 4^2 \equiv_g 5^2$

1. $4 \equiv_g 49 \quad L = [25, 7, 263, 5, 153, 35, 221, 1]$
2. $5 \equiv_g 50 \quad L = [25, 7, 263, 5, 17, 35, 221, 1]$

$(\ldots) \quad L = [1, 1, 263, 1, 17, 1, 221, 1]$

$$75 = 3 \cdot 5^2$$
$$168 = 2^3 \cdot 5 \cdot 7$$
$$360 = 2^3 \cdot 3^2 \cdot 5$$
$$560 = 2^4 \cdot 5 \cdot 7$$
$$768 = 2^8 \cdot 3$$

$$\begin{array}{c} \\ 75 \\ 2 \\ 3 \\ 5 \\ 7 \end{array}\begin{array}{c} \begin{array}{ccccc} 46 & 47 & 49 & 51 & 53 \\ 168 & 360 & 560 & 768 & \end{array} \\ \begin{pmatrix} 0 & 3 & 3 & 4 & 8 \\ 1 & 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \end{array} =: M$$

$$\ker(M \bmod 2) = \ker\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$$= \left\langle \underbrace{\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

$$\Rightarrow y \equiv_N \sqrt{75 \cdot 168 \cdot 360 \cdot 560} \equiv_N 1416$$

$$x \equiv_N 46 \cdot 47 \cdot 49 \cdot 51 \equiv_N 311$$

$$ggT(1416 - 311, N) = 13$$

$$\boxed{2041 = 13 \cdot 157}$$