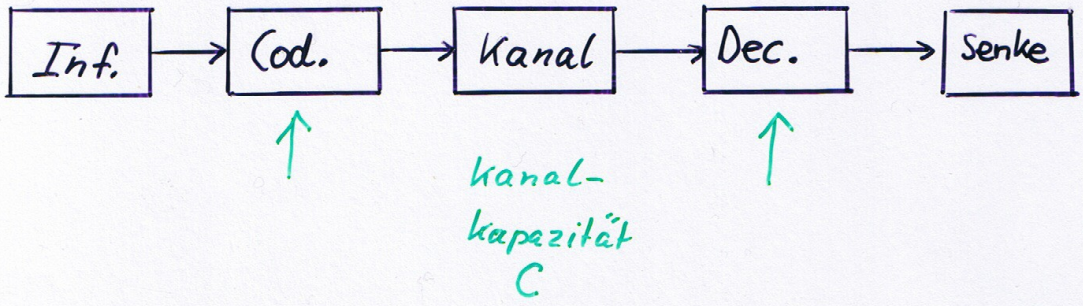
Zusammenfassung vom 17.10.2014



Mit Codierung kann man sich C nähern.

Blockcodes: Menge von Codewörtern, die voneinander möglichst großen Abstand haben.

(n, M, d) – Code über geeignetem Alphabet (mit q Elementen)

n: Länge, M: Anzahl der CW, d: Mindestdistanz

Lineare Codes: $[n, k, d]$-Codes $\quad k = \log_q M$

Summe von Codewörtern ergibt wieder Codewort.

k: Anzahl der Informationsstellen, Dimension

$R = \frac{k}{n}$ Coderate

Zur Beschreibung von linearen Codes

Generatormatrix: $\underline{G} = \begin{pmatrix} \text{Basis von} \\ \text{Codewörtern} \end{pmatrix}$

Günstige Form: $\underline{G} = (\underline{I}_k \mid \underline{P})$

Prüfmatrix: $\underline{H} = (-\underline{P}^T \mid \underline{I}_{n-k})$

$\underline{c} = \underline{m} \cdot \underline{G}$ ↑ Codierung

$\underline{H} \cdot \underline{c}^T = \underline{0}$ ↑ Test ob Vektor CW ist

Decodierung: $\underline{r} = \underline{c} + \underline{e}$

$$\underline{H} \cdot \underline{r}^T = \underline{H} \cdot (\underline{c}^T + \underline{e}^T) = \underline{H} \cdot \underline{e}^T$$

Syndrom: $\underline{s}^T = \underline{H} \cdot \underline{e}^T$

Zusammenfassung vom 17.10.2014

$GF(q)$: endlicher Körper mit q Elementen

$q = p^m$ ← Primzahlpotenz

Konstruktion mit irreduziblem Polynom $p(x)$. (Koeff. $\in GF(p)$, Grad $= m$)

Besonders "beliebtes" Polynom: primitives Polynom

→ NS ist primitiv. $p(\alpha) = 0$

$$\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}\} = GF(q) \setminus \{0\}$$

Man sagt α hat die Ordnung $q-1$, $\alpha^{q-1} = 1$.

Jeder endliche Körper besitzt mindestens ein primitives Element.

α ist Wurzel von $x^q - x$

⇒ Jedes Element von $GF(q)$ ist Wurzel von $x^q - x$, denn es gilt $(\alpha^i)^q - \alpha^i = (\alpha^q)^i - \alpha^i = \alpha^i - \alpha^i = 0$.

⇒ Das Polynom $x^q - x$ enthält alle Elemente von $GF(q)$ als Nullstellen.

Außerdem: Die Gleichung $x^q = x$ kann benutzt werden um zu testen ob ein Element dem Körper $GF(q)$ angehört.

Hamming Code [7, 4, 3]

$$\underline{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Beschreibung mit $GF(2^3)$

$$\underline{\tilde{H}} = \left(\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\right)$$

$$= \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$GF(2^3)$
0 0 1
0 1 0
1 0 0
0 1 1
1 1 0
1 1 1
1 0 1

Nur die Reihenfolge der Spalten hat sich geändert!

$$\underline{\tilde{H}} \cdot \underline{c}^T = \underline{\tilde{H}} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0$$

$$\Rightarrow \sum_{i=0}^{n-1} c_i \alpha^i = 0$$

Darstellung des Codewortes $\underline{c}$ als Polynom $c(x)$.

Ebenso: $\underline{r} \leftrightarrow r(x)$ und $\underline{e} \leftrightarrow e(x)$.

Codewortpolynom: $C(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$

Es gilt: $C(\alpha) = 0$ $\quad c_i \in \{0,1\} = GF(2)$

Idee: $C(x) = i(x) \cdot (x-\alpha)$ ← Problem: $C(x)$ soll über $GF(2)$ sein, aber $\alpha \in GF(2^3)$

Deshalb: Suche binäres Polynom, das α als Nullstelle enthält!

Lösung: Bereits bekannt ⇒ das primitive Polynom mit dem $GF(2^3)$ konstruiert wurde. $g(x) = x^3 + x + 1 \stackrel{!}{=} p(x)$

$g(x)$ ist das sogenannte Generatorpolynom

$$C(x) = \underbrace{i(x)}_{\text{Grad 3}} \cdot \underbrace{g(x)}_{\text{Grad 3}}$$

↳ 2^4 Möglichkeiten

Informationspolynom: $i(x)$, Grad $= k-1$

Generatorpolynom: $g(x)$, Grad $= n-k$

Hausaufgabe

Decodieren Sie $\underline{r}(x) = x^4 + x^2 + x$ und $r(x) = x^5 + x$

zum nächsten Codewort ($H = (\alpha^0, \alpha^1, \ldots, \alpha^6)$

$p(x) = x^3 + x + 1$; $p(\alpha) = 0$)

Ziel: 2 Fehlerkorrektur

$$\underline{H} = \begin{pmatrix} \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1} \\ \hline f(\alpha^0), f(\alpha^1), f(\alpha^2), \ldots, f(\alpha^{n-1}) \end{pmatrix}$$

$n = 2^m - 1$

α: primitives Element von $GF(2^m)$.

$f: GF(2^m) \to GF(2^m)$

H-Matrix ist eine $2m \times n$ Matrix.

1. Idee: $f(z) = z^2$

$r(x) = c(x) + e(x)$

$e(x) = x^{j_1} + x^{j_2}$

$$S_1 = r(\alpha) = \underbrace{c(\alpha)}_{=0} + e(\alpha) = \alpha^{j_1} + \alpha^{j_2}$$

$$S_2 = r(\alpha^2) = c(\alpha^2) + e(\alpha^2) = \alpha^{2j_1} + \alpha^{2j_2}$$

Schlechte Idee, da gilt $S_1^2 = \alpha^{2j_1} + \underbrace{2\alpha^{j_1+j_2}}_{=0} + \alpha^{2j_2} = S_2$

S_2 bringt keine neue Erkenntnis!

2. Idee: $f(z) = z^3$

$$\underline{H} = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \dots & \alpha^{n-1} \\ \alpha^0 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \end{pmatrix}$$

$$S_1 = r(\alpha) = \alpha^{i_1} + \alpha^{i_2} = x_1 + x_2$$
$$S_3 = r(\alpha^3) = \alpha^{3i_1} + \alpha^{3i_2} = x_1^3 + x_2^3$$

$$\Rightarrow \quad S_1^3 = x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3$$

$$S_1^3 = S_3 + x_1 x_2 (x_1 + x_2)$$

$$S_1^3 = S_3 + x_1 x_2 \cdot S_1$$

$$S_1^3 = S_3 + x_1 (S_1 + x_1) S_1$$ ← ebenso für x_2

$$x_1^2 S_1 + x_1 S_1^2 + S_1^3 + S_3 = 0$$

$$x_1^2 + S_1 x_1 + \frac{S_1^3 + S_3}{S_1} = 0$$ ↓ gl. Gl. für x_2

$$\Rightarrow \quad \boxed{z^2 + S_1 z + \left(S_1^2 + \frac{S_3}{S_1}\right) = 0}$$

Lösen von quadratischen Gleichungen in $GF(2^m)$

$$a y^2 + by + c = 0 \qquad a, b, c \in GF(2^m)$$

$a \neq 0,\ b \neq 0,\ c \neq 0$

zunächst: setze $y = bx/a$

$$\rightsquigarrow \quad a b^2 \frac{x^2}{a^2} + \frac{b^2 x}{a} + c = 0$$

$$\Rightarrow \quad x^2 + x + \frac{ac}{b^2} = 0$$

$$\Rightarrow \text{Löse:} \quad x^2 + x + \gamma = 0 \qquad (*)$$

Wenn x_1 eine Lösung von $(*)$ ist

$\Rightarrow x_2 = x_1 + 1$ ist die zweite Lösung

denn $(x_1+1)^2 + (x_1+1) + \gamma = x_1^2 + 1 + x_1 + 1 + \gamma$

$$= x_1^2 + x_1 + \gamma \overset{!}{=} 0$$

$$x^2 + x + \gamma = 0 \qquad \gamma \in GF(2^m)$$

$$x^{2^2} + x^2 + \gamma^2 = 0$$

$$x^{2^3} + x^{2^2} + \gamma^{2^2} = 0$$

$$\vdots$$

$$x^{2^m} + x^{2^{m-1}} + \gamma^{2^{m-1}} = 0$$

Summe: $x^{2^m} + x + tr(\gamma) = 0$

$x^{2^m} = x$ im $GF(2^m)$ $\Rightarrow$ $tr(\gamma) = 0$

Damit $x^2 + x + \gamma$ zwei Nullstellen in $GF(2^m)$ hat muß gelten: $tr(\gamma) = 0$

Wenn $\gamma \in GF(2^m)$, dann gilt

$$tr(\gamma) = 0 \quad \text{oder} \quad tr(\gamma) = 1$$

Die Hälfte der Elemente von $GF(2^m)$ hat die Spur (trace) 1 und die Hälfte die Spur 0.

$\rightarrow$ Lösungen von $x^{2^{m-1}} + x^{2^{m-2}} + \dots + x^2 + x = \begin{cases} 0 \\ 1 \end{cases}$.

Suche ein Element $u \in GF(2^m)$ mit $tr(u) = 1$.

Die Lösung x_1 von $x^2 + x + \gamma = 0$ ist dann gegeben durch:

$$x_1 = \gamma \cdot u^2 + (\gamma + \gamma^2) u^{2^2} + \dots + (\gamma + \gamma^2 + \dots + \gamma^{2^{m-2}}) u^{2^{m-1}}$$

Beweis: Durch Einsetzen $\rightarrow$ Hausaufgabe

Für m ungerade gilt: $tr(1) = 1 \Rightarrow$ Vereinfachung

$$x_1 = \gamma^2 + \gamma^{2^3} + \dots + \gamma^{2^{m-2}} \qquad m \text{ ungerade}$$

Die Formeln sind algorithmisch sehr effizient

(auch für sehr große Körper!)

Beispiel für 2-Fehler korrigierenden Code

Bin. [15, 7, 5] BCH-Code ← Def. folgt später

$$H = \begin{pmatrix} \alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \dots, \alpha^{14} \\ \alpha^0, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}, \alpha^{15}, \alpha^{18}, \dots, \alpha^{3\cdot 14} \end{pmatrix}$$

$\alpha^{15} = 1$

α : prim. Element von $GF(2^4)$ $\quad p(\alpha) = 0$ mit $p(x) = x^4 + x + 1$

$c(\alpha) = 0 \Rightarrow c(x)$ ist Vielfaches von $x^4 + x + 1$

$c(\alpha^3) = 0 \Rightarrow c(x)$ ist Vielfaches des

Minimalpolynoms von α^3.

(binären) Minimalpolynom von α^3 :
- Enthält α^3 als Wurzel
- Koeffizienten aus GF(2)
- Polynom kleinsten Grades, das α^3 als Wurzel hat.

Sei $m_i(x)$ Minimalpolynom von $\alpha^i \Rightarrow \alpha^{2i}, \alpha^{2^2 i}, \dots$

sind ebenfalls Nullstellen von $m_i(x)$

folgt aus $m_i(x)^2 = m_i(x^2)$

im Allgemeinfall (p statt 2): $m(x)^p = m(x^p)$.

Berechnung des Minimalpolynoms von α^3:

α^3 Nullstelle $\Rightarrow$ α^6, α^{12}, $\alpha^{24} = \alpha^9$ sind ebenfalls Nullstellen. ($\alpha^{18} = \alpha^3$ ↑ Schon in Liste)

$$m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12})$$

$$= (x^2 + (\alpha^3+\alpha^6)x + \alpha^9) \cdot (x^2 + (\alpha^9+\alpha^{12})x + \alpha^6)$$

$$= x^4 + \underbrace{(\alpha^3+\alpha^6+\alpha^9+\alpha^{12})}_{=1} x^3$$
$$+ (\alpha^6 + \alpha^9 + (\alpha^3+\alpha^6)(\alpha^9+\alpha^{12}))\, x^2$$
$$+ ((\alpha^3+\alpha^6)\alpha^6 + (\alpha^9+\alpha^{12})\alpha^9)\, x$$
$$+ \underbrace{\alpha^{15}}_{1}$$

$$= x^4 + x^3 + (\overbrace{\alpha^6+\alpha^8+\alpha^{12}+\cancel{\alpha^{15}}+\cancel{\alpha^{15}}+\alpha^3}^{1})\, x^2$$
$$+ \underbrace{(\alpha^9+\alpha^{12}+\alpha^3+\alpha^6)}_{=1} x + 1$$

$$\Rightarrow m_3(x) = x^4 + x^3 + x^2 + x + 1$$

$$m_1(x) = p(x) = x^4 + x + 1$$

$\Rightarrow$ **Generatorpolynom:** $g(x) = m_1(x)\, m_3(x)$

$\Rightarrow g(x) =$ H. A.

Annahme: zwei Bitfehler sind aufgetreten

$$e(x) = x^7 + x^{11}$$

der Einfachheit halber: $C(x) = 0$

$$\Rightarrow r(x) = x^7 + x^{11}$$

$$\Rightarrow S_1 = r(\alpha) = \alpha^7 + \alpha^{11} = \alpha^8 \quad \leftarrow \text{siehe Tabelle}$$

$$S_3 = r(\alpha^3) = \alpha^{21} + \alpha^{33} = \alpha^6 + \alpha^3 = \alpha^2$$

Einsetzen in: $z^2 + S_1 z + \left(S_1^2 + \frac{S_3}{S_1}\right) = 0$

Führt zu: $z^2 + \alpha^8 z + \left(\alpha + \alpha^{2-8}\right) = 0$

$$z^2 + \alpha^8 z + \left(\alpha + \alpha^9\right) = 0$$

$$z^2 + \alpha^8 z + \alpha^9 = 0 \qquad (*)$$

Lösung: α^7 und α^{11} $\Rightarrow e(x) = x^7 + x^{11}$

H.A.: Lösen Sie (*) mit der quadratischen Lösungsformel

BCH - Codes

α : primitives Element aus $GF(p^m)$

$n = p^m - 1$

Def. durch Prüfmatrix

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{(\delta-1)2} & \cdots & \alpha^{(\delta-1)(n-1)} \end{pmatrix}$$

Zyklischer Code mit

Generatorpolynom $g(x) = kgV$ der $m_j(x)$

$j = 1, 2, \ldots \delta-1$

$m_j(x)$: Minimalpolynom von α^j

↳ Da Generatorpolynom hat die Nullstellen $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$.

δ nennt man die entworfene Distanz.

BCH Schranke: Für die tatsächliche Mindestdistanz d des durch $g(x)$ definierten Codes gilt $d \geq \delta$

Beweis: Damit H Prüfmatrix eines Codes mit der Mindestdistanz d ist, müssen je $d-1$ Spalten linear unabhängig sein.

Bedingung

$$\Leftrightarrow \operatorname{Det}\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \cdots & \alpha^{2i_{\delta-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(\delta-1)i_1} & \alpha^{(\delta-1)i_2} & \cdots & \alpha^{(\delta-1)i_{\delta-1}} \end{pmatrix} \neq 0$$

Setze $X_1 = \alpha^{i_1}, X_2 = \alpha^{i_2}, \ldots, X_{\delta-1} = \alpha^{i_{\delta-1}}$

Vandermonde Matrix

$$\Rightarrow \operatorname{Det}\begin{pmatrix} X_1 & X_2 & \cdots & X_{\delta-1} \\ X_1^2 & X_2^2 & \cdots & X_{\delta-1}^2 \\ \vdots & \vdots & & \vdots \\ X_1^{\delta-1} & X_2^{\delta-1} & \cdots & X_{\delta-1}^{\delta-1} \end{pmatrix}$$

$$= X_1 \cdot X_2 \cdot \ldots X_{\delta-1} \cdot \operatorname{Det}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_{\delta-1} \\ \vdots & \vdots & & \vdots \\ X_1^{\delta-2} & X_2^{\delta-2} & \cdots & X_{\delta-1}^{\delta-2} \end{pmatrix}$$

$$= X_1 \cdot X_2 \cdot \ldots X_{\delta-1} \cdot \prod_{i>j} (X_i - X_j) \neq 0$$ wenn alle X_j verschieden!

Parameter der BCH-Codes

$[n, k, d]$ Codes über $GF(p)$

$n = p^m - 1$

$d \geq \delta$ ($\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ sind Nullstellen von $g(x)$)

$k = n - \text{Grad}\{g(x)\}$

Die Bestimmung des Grades von $g(x)$ erfolgt mit den sogenannten Kreisteilungsklassen (cyclotomic Cosets).

Beispiel: $n = 2^m - 1$; $m = 4$; $\delta = 5$

α NS von $g(x)$ $\rightarrow \alpha^2, \alpha^{2^2} \dots \alpha^{2^{m-1}}$ NS von $g(x)$

$C_1 = \{1, 2, 4, 8\}$ ← solange mit $p=2$ Multiplizieren mod 2^m-1 bis Anfangswert wieder auftaucht

bisher $\delta = 3$

$C_3 = \{3, 6, 12, 9\}$

$C_1 \cup C_3 = \{1, 2, 3, 4, 6, \dots\}$

jetzt $\delta = 5$ ✓

Anzahl der Prüfstellen: $|C_1 \cup C_3| = 8$.

Weiteres Beispiel: $n = 2^6 - 1 = 63$

$C_1 = \{1, 2, 4, 8, 16, 32\}$

$C_3 = \{3, 6, 12, 24, 48, 33\}$

$96 \bmod 63 = 33$

$C_5 = \{5, 10, 20, 40, 17, 34\}$

$80 \bmod 63 = 17$

$C_7 = \{7, 14, 28, 56, 49, 35\}$

$112 \bmod 63 = 49$

Sei $g(x) = m_1(x) \cdot m_3(x) \cdot m_5(x) \cdot m_7(x)$

$\Rightarrow \delta = 9 \Rightarrow d \geq 9 \rightsquigarrow [63, 39, 9]$-Code

bzw ≥ 9

$C_9 = \{9, 18, 36\}$

Sei $g(x) = m_1(x) \cdot m_3(x) \cdot m_5(x) \cdot m_7(x) \cdot m_9(x)$

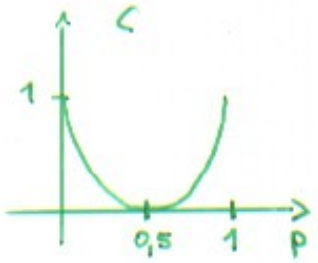
$\Rightarrow \delta = 11 \Rightarrow d \geq 11 \rightsquigarrow [63, 36, 11]$-Code

bzw ≥ 11

Hausaufgabe: Bestimmen Sie die Parameter $[511, k, d]$ aller binären BCH-Codes mit $\delta \leq 11$.

Lösung Übungsaufgaben

1.) $C = 1 + p \operatorname{ld} p + (1-p) \operatorname{ld}(1-p)$



2.) Mindestdistanz des mit

$$\underline{G} = \begin{pmatrix} 1000 & 011 \\ 0100 & 101 \\ 0010 & 110 \\ 0001 & 111 \end{pmatrix}$$

erzeugten Codes

Inf.	→ Prüfbits	Gew.
0000	000	0
1000	011	3
0100	101	3
1100	110	4
0010	110	3
1010	101	4

etc.

Linearer Code

⇒ Mindestdistanz = Mindestgew.

⇒ $d = 3$

$[7,4,3]$-Code

3.) Generator und Prüfmatrix des $[n,1,n]$ Codes

$$\underline{G} = (1 \mid \underbrace{1 1 1 \ldots 1 1}_{n-1 \text{ Einsen}}) \qquad \underline{H} = \begin{pmatrix} 1 & 1 & 0 & 0 \ldots & 0 \\ 1 & 0 & 1 & 0 \ldots & 0 \\ \vdots & & & & \\ 1 & 0 & \ldots\ldots & & 1 \end{pmatrix}$$

4.) $\underline{G}$ und $\underline{H}$ von $[n,n-1,2]$ Code

$$\underline{G} = \begin{pmatrix} 1 & 0 \ldots & 0 & 1 \\ 0 & 1 & & 1 \\ & \ddots & & \vdots \\ 0 & \ldots & 0 1 & 1 \end{pmatrix} \qquad \underline{H} = (\underbrace{1 1 \ldots 1 1}_{n-1 \text{ Einsen}} 1)$$

$= I_{n-1}$

5.) $V_t = 1 + \binom{n}{1} + \binom{n}{2} t \ldots + \binom{n}{t}$ ← V_t für Binärcodes

1 ↑ CW; $\binom{n}{1}$ ↑ Gew. = 1; $\binom{n}{2}$ ↑ Gew. = 2; $\binom{n}{t}$ ↑ Gew. = t

6.)

C++ Programm zur Berechnung des ggT

z.B. GNU C++ Compiler. Mit **typedef long long integer;**

hat man eine 64 Bit ganze Zahl zur Verfügung, die für fast alle Zwecke der Vorlesung genügt

Der Euklidsche Algorithmus

Eingabeparameter: m und n.

Ausgabewert: Der größte gemeinsame Teiler von m und n.

Aufruf: ggT(m,n)

```
integer ggT(const integer& m,const integer& n)
        {
         integer rr[2]={m,n};
         int i;
         for (i=0; rr[1-i]!=0;i=1-i) rr[i]%=rr[1-i];
        return rr[i];
        }
```

Der erweiterte Euklidsche Algorithmus

Eingabeparameter: m und n.

Ausgabeparameter: Werte ggt, q und p für die gilt ggt = q m + p n

Aufruf: eea(m,n,ggt,q,p)

```
void eea(const integer& m,const integer& n,integer& ggt, integer& q, integer& p)
        {
         integer qq[2]={1,0};
         integer pp[2]={0,1};
         integer rr[2]={m,n};
         int i;
         integer a;
         for (i=0; rr[1-i]!=0;i=1-i)
          {
            a=rr[i]/rr[1-i];
            rr[i]=rr[i] - a*rr[1-i];
            qq[i]=qq[i] - a*qq[1-i];
            pp[i]=pp[i] - a*pp[1-i];
          }
        ggt=rr[i];
        q  =qq[i];
        p  =pp[i];
        }
```

Aufgabe 7: Konstruieren Sie den Körper $GF(2^4)$.

$p(x) = x^4 + x + 1$ ← primitives Polynom

$p(\alpha) = 0 \Rightarrow \alpha^4 + \alpha + 1 = 0 \qquad \alpha^4 = \alpha + 1$

i	α^i	α^3	α^2	α^1	α^0
0	1	0	0	0	1
1	α	0	0	1	0
2	α^2	0	1	0	0
3	α^3	1	0	0	0
4	α^4	0	0	1	1
5	α^5	0	1	1	0
6	α^6	1	1	0	0
7	α^7	1	0	1	1
8	α^8	0	1	0	1
9	α^9	1	0	1	0
10	α^{10}	0	1	1	1
11	α^{11}	1	1	1	0
12	α^{12}	1	1	1	1
13	α^{13}	1	1	0	1
14	α^{14}	1	0	0	1

Aufgabe 8: Konstruieren Sie den Körper $GF(3^2)$

Benötigt wird ein irreduzibles oder besser ein primitives Polynom vom Grad 2 über $GF(3)$

irred. Polynom vom Grad 1: x, $x+1$, $x+2$

$\Rightarrow$ $(x+1)^2 = x^2+2x+1$ ist reduzibel

$(x+2)^2 = x^2+x+1$ " "

$(x+1)(x+2) = x^2+2$ " "

aber x^2+1 ist irreduzibel

$p(x) = x^2+1$ $\quad p(\alpha) = 0 \rightsquigarrow \alpha^2+1=0 \quad \alpha^2=-1$

$(\alpha = i)$

i	α^i	α	1	
0	1	0	1	
1	α	1	0	
2	α^2	0	2	$\leftarrow$ $\alpha^2 = -1 \equiv 2 \bmod 3$
3	α^3	2	0	$2\alpha^2 = 1$
4	α^4	0	1	

$GF(3^2)$ enthält $3^2-1=8$ von Null verschiedene Elemente. Polynom x^2+1 ist irreduzibel aber nicht primitiv!

Neuer Versuch mit $p(x) = x^2 + x + 2$

$\alpha^2 + \alpha + 2 = 0 \quad \leadsto \alpha^2 = 2\alpha + 1$

j	α^j	α	1
0	1	0	1
1	α	1	0
2	α^2	2	1
3	α^3	2	2
4	α^4	0	2
5	α^5	2	0
6	α^6	1	2
7	α^7	1	1

$\alpha^8 = 1$

$\leftarrow \alpha^3 = 2\alpha^2 + \alpha = 2(2\alpha+1) + \alpha$
$= 2\alpha + 2$

$\alpha^4 = 2\alpha^2 + 2\alpha$
$= 2(2\alpha+1) + 2\alpha = 2$

$\Rightarrow p(x)$ ist primitives Polynom.