

Informationsverarbeitung
Prüfzeichen-Verfahren

DIN
ISO 7064

Data processing; check character systems

Traitement des données; systèmes de caractères de contrôle

Die Internationale Norm ISO 7064, 1. Ausgabe 1983-09-15, ist in diese Deutsche Norm unverändert übernommen worden.

Nationales Vorwort

a) Die Internationale Norm gliedert sich in folgende Abschnitte:

	Seite		Seite
Vorwort	2	5.3 Die Stelle für die Prüfzeichen	5
0 Einleitung	3	6 Rechenmethoden für reine Verfahren mit einem Prüfzeichen	6
1 Anwendungsbereich	3	6.1 Die rekursive Methode	6
Hauptabschnitt eins: Allgemeines		6.2 Die Polynom-Methode	7
2 Begriffe	3	7 Rechenmethoden für reine Verfahren mit zwei Prüfzeichen	8
3 Arten von Verfahren	4	Hauptabschnitt drei: Gemischte Verfahren	
3.1 Reine Verfahren	4	8 Beschreibung der gemischten Verfahren	9
3.2 Gemischte Verfahren	4	9 Die Rechenmethode für gemischte Verfahren	9
4 Normkonformität und Produktbezeichnung	4	Anhang A. Kriterien für die Auswahl eines Prüfzeichen-Verfahrens für die Anwendung	10
Hauptabschnitt zwei: Reine Verfahren		Anhang B. Prüfzeichen-Verfahren für andere Alphabete	12
5 Beschreibung der reinen Verfahren	5		
5.1 Die Formel	5		
5.2 Rechengang	5		

b) Zu Abschnitt 0:

ISO 2108 – 1978 Documentation – International standard book numbering (ISBN)

ISO 2894 – 1980 Embossed credit cards – Specifications, numbering system and registration procedure

ISO 6166 – 1981 Bank operations – International securities identification numbering system

Im Original wird irrtümlich ISO 2984 statt ISO 2894 genannt.

Zu den zitierten ISO-Normen existieren folgende Deutsche Normen:

DIN 1462 Internationales Standardbuchnummern-System (ISBN)

DIN 9781 Teil 1*) Büro- und Datentechnik; Identifikationskarten aus Kunststoff oder kunststofflaminiertem Werkstoff; Anforderungen an die Identifikationskarte 1 (ID 1)

DIN 9781 Teil 2*) Büro- und Datentechnik; Identifikationskarten aus Kunststoff oder kunststofflaminiertem Werkstoff; Darstellung von Daten auf der Identifikationskarte 1 (ID 1), Übersicht

c) Zu Abschnitt 8.1:

Im Original steht in der Zeichenerklärung a anstelle von a_i .

d) Zu Abschnitt 9.1.1:

In der letzten Zeile steht im Original nur $P_n + a_1 \equiv 1 \pmod{M}$. Die vorliegende Fassung enthält die richtige Formel.

e) Zum Anhang A:

Die angebliche Fehlerklasse 6 ist tatsächlich der Mittelwert aus allen Fehlerklassen 1 bis 5 und wäre daher eigentlich unter e) – der Restfehler – aufzuführen.

f) Zu Tabelle 5, Spalte 7, Verfahren ISO 7064, MOD 37-2:

Im Original ist irrtümlich der Prüfzeichenwert 10 anstelle von 36 genannt.

g) Zum Anhang B:

Das Beispiel gilt sinngemäß auch für ein um die Umlaute Ä, Ö und Ü erweitertes deutsches Alphabet.

*) Das in ISO 2894 – 1980, Anhang E, beschriebene Luhn-Verfahren ist in DIN 9781 Teil 1 und Teil 2 nicht enthalten.

Fortsetzung Seite 2 bis 12

Deutsche Übersetzung

Falls bei Verhandlungen mit englisch- oder französischsprachigen Partnern Zweifelsfälle auftreten, ist die entsprechende Originalfassung der Internationalen Norm heranzuziehen.

Internationale Norm ISO 7064–1983

Informationsverarbeitung

Prüfzeichen-Verfahren

Vorwort

Die ISO (Internationale Normungsorganisation) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitglieds-körperschaften). Die Erarbeitung internationaler Normen obliegt den Technischen Komitees der ISO. Jede Mitgliedskörper-schaft, die sich für ein Thema interessiert, für das ein Technisches Komitee eingesetzt wurde, ist berechtigt, in diesem Komitee mitzuarbeiten. Internationale (staatliche und nichtstaatliche) Organisationen, die mit der ISO in Verbindung stehen, sind an den Arbeiten ebenfalls beteiligt.

Die von einem Technischen Komitee verabschiedeten Entwürfe für internationale Normen werden den Mitgliedskörperschaf-ten zunächst zur Genehmigung vorgelegt, bevor sie vom Rat der ISO als Internationale Norm angenommen werden.

Die Internationale Norm ISO 7064 wurde vom Technischen Komitee ISO/TC 97 „Informationsverarbeitungssysteme“ erarbeitet und im November 1981 an die Mitgliedskörperschaften versandt.

Sie wurde von den Mitgliedskörperschaften folgender Länder angenommen:

Ägypten	Irland	Schweiz
Belgien	Italien	Spanien
China	Japan	Südafrika
Dänemark	Niederlande	Tschechoslowakei
Deutschland, Bundesrepublik	Polen	Vereinigtes Königreich
Finnland	Rumänien	Vereinigte Staaten
Frankreich	Schweden	

Keine Mitgliedskörperschaft äußerte irgendwelche Einwände gegen diese Norm.

0 Einleitung

Der Bedarf nach einer Normung von Prüfzeichen-Verfahren ergibt sich aus folgenden Überlegungen:

- a) Es sind 100 oder mehr Verfahren in Gebrauch, viele davon haben fast identische Eigenschaften, und eine derartige Vielfalt bietet keine erkennbaren Vorteile;
- b) nur wenige von diesen Verfahren wurden mathematisch völlig durchgeprüft, manche von ihnen enthalten schwerwiegende Mängel;
- c) die Vielfalt der Verfahren beeinträchtigt die Wirtschaftlichkeit bei der Herstellung von Geräten zur Berechnung oder Prüfung der Prüfzeichen, und oft verhindert sie die Prüfung von ausgetauschten Daten.

Aus diesem Grunde wurde eine kleine Anzahl von Verfahren ausgewählt, entsprechend den unterschiedlichen Bedürfnissen der Anwendung; sie sind mathematisch geprüft, und innerhalb seines Anwendungsbereiches bietet jedes von ihnen die höchstmögliche Sicherheit gegen typische Abschreib- und Eintastfehler.

Weitere Prüfzeichen-Verfahren für spezielle Anwendungsbereiche sind in ISO 2108, ISO 2894 und ISO 6166 festgelegt *). Sie erreichen jedoch nicht die Fehlererkennungsrate der hier beschriebenen Verfahren.

Anhang A faßt die Kriterien zusammen, die zu beachten sind bei der Auswahl eines Prüfzeichen-Verfahrens für eine bestimmte Anwendung.

Anhang B erläutert, wie man weitere, auf diese Norm aufbauende Prüfzeichen-Verfahren für nationale Alphabete entwickeln kann, die von dem international verwendeten 26-Buchstaben-Alphabet abweichen, für das die Verfahren dieser Norm entwickelt wurden.

1 Anwendungsbereich

1.1 Diese Norm definiert eine Anzahl von Prüfzeichen-Verfahren zur Sicherung von Zeichenketten gegen Fehler, die auftreten, wenn Daten von Menschen abgeschrieben oder in Tastaturen eingegeben werden. Die Zeichenketten können festes oder variables Format haben und aus einem der folgenden Zeichenvorräte stammen:

- a) numerisch (10 Ziffern: 0 bis 9)
- b) alphabetisch (26 Buchstaben: A bis Z)
- c) alphanumerisch (Buchstaben und Ziffern).

Auftretende Zwischenräume und Sonderzeichen bleiben unberücksichtigt.

1.2 Diese Norm legt die Anforderungen für Produkte fest, von denen angegeben wird, daß sie Prüfzeichen erzeugen oder Zeichenketten prüfen entsprechend den hier genormten Verfahren.

1.3 Die beschriebenen Prüfzeichen-Verfahren erkennen folgende Fehler:

- a) alle einfachen Substitutionsfehler (Ersatz eines einzelnen Zeichens durch ein anderes, z. B. 4234 statt 1234)
- b) alle oder nahezu alle einfachen Transpositionsfehler (Vertauschen zweier einzelner Zeichen, sowohl benachbarter als auch mit einem Zeichen dazwischen, z. B. 12354 oder 12543 anstatt 12345)
- c) alle oder nahezu alle Verschiebungsfehler (Verschieben einer ganzen Zeichenkette nach links oder rechts, z. B. _ 1 2 3 statt 1 2 3 _)
- d) einen hohen Anteil von doppelten Substitutionsfehlern (zwei verschiedene einfache Substitutionsfehler in der gleichen Zeichenkette, z. B. 7234587 anstatt 1234567)
- e) einen hohen Anteil von allen anderen Fehlern.

1.4 Diese Norm enthält keine spezifischen Verfahren für folgende Aufgaben:

- a) Fehlererkennung mit eingeschlossener automatischer Korrektur
- b) Erkennung von beabsichtigten Verfälschungen
- c) Prüfung von Zeichenketten, die nur zwischen Maschinen ausgetauscht werden.

1.5 Diese Norm soll dem Informationsaustausch zwischen Organisationen dienen; sie ist aber auch für interne Informationssysteme nützlich und sehr empfehlenswert.

Hauptabschnitt eins – Allgemeines

2 Begriffe

2.1 Prüfzeichen (check character): Ein zur Zeichenkette hinzugefügtes Zeichen, das, über eine mathematische Beziehung zur Kette, zur Prüfung der Richtigkeit der Zeichen verwendet werden kann.

2.2 Prüfzeichen-Verfahren (check character system): Die Gesamtheit der Regeln für die Berechnung der Prüfzeichen und die Prüfung der so ergänzten Zeichenketten.

2.3 Zusatzzeichen (supplementary character; supplementary check character): Ein nur als Prüfzeichen verwendetes Zeichen, das nicht zum Zeichenvorrat der zu sichernden Kette gehört.

2.4 Modul (modulus): Eine ganze Zahl, die als Divisor für einen ganzzahligen Dividenden verwendet wird, um einen ganzzahligen Rest zu erzeugen.

*) Siehe Nationales Vorwort

2.5 Kongruenz (congruence): Die Eigenschaft einer Menge von ganzen Zahlen, deren Differenzen ganze Vielfache des Moduls sind. Bezeichnet wird die Kongruenz durch das Symbol $\equiv$.

Beispiel: $39 \equiv 6 \pmod{11}$ bedeutet, daß 39 und 6 kongruent sind bezüglich des Moduls 11, d. h. $39 - 6 = 33$ ist ein Vielfaches von 11.

2.6 Basis (radix): Die Basis einer geometrischen Zahlenfolge.

3 Arten von Verfahren

Diese Norm enthält zwei Arten von Verfahren:

- a) reine Verfahren
- b) gemischte Verfahren

3.1 Reine Verfahren

Die reinen Verfahren sind aufgelistet in Tabelle 1 und festgelegt in Hauptabschnitt zwei:

Jedes reine Verfahren verwendet einen einzigen Modul für sämtliche Rechenschritte.

Tabelle 1. **Reine Verfahren**

Bezeichnung ¹⁾ des Prüfzeichen-Verfahrens	Anwendung	Anzahl und Art der Prüfzeichen ²⁾
ISO 7064, MOD 11-2 ISO 7064, MOD 37-2	Ziffernketten alphanumerische Ketten	1 Ziffer oder Zusatzzeichen X 1 Ziffer oder Buchstabe oder Zusatzzeichen *
ISO 7064, MOD 97-10 ISO 7064, MOD 661-26 ISO 7064, MOD 1271-36	Ziffernketten Buchstabenketten alphanumerische Ketten	2 Ziffern 2 Buchstaben 2 Ziffern oder Buchstaben
¹⁾ In dieser Bezeichnung ist die erste Zahl hinter ‚MOD‘ der Modul, die zweite Zahl die Basis. ²⁾ Die ersten beiden Verfahren können ein Zusatzzeichen erzeugen, das nicht im Zeichenvorrat der zu prüfenden Ketten enthalten ist (d. h. für ISO 7064, MOD 11-2 erscheint als Prüfzeichen eine Ziffer von 0 bis 9 oder X; für ISO 7064, MOD 37-2 erscheint eine der Zeichen 0 bis 9, A bis Z oder *). Wo das Zusatzzeichen nicht zulässig ist und nur ein Prüfzeichen verwendet werden kann, könnte man jene Zeichenketten vermeiden, die das Zusatzzeichen erzeugen. Wenn man weder das Zusatzzeichen verwenden, noch die entsprechenden Zeichenketten vermeiden kann, dann kann man auf ein gemischtes Verfahren ausweichen.		

3.2 Gemischte Verfahren

Die gemischten Verfahren sind aufgelistet in Tabelle 2 und festgelegt in Hauptabschnitt drei.

Jedes gemischte Verfahren verwendet in der Rechnung zwei Moduln. Der eine Modul ist gleich der Anzahl der Zeichen im Zeichenvorrat, der andere Modul ist um eins größer. Diese gemischten Verfahren erzeugen immer ein Prüfzeichen aus dem Zeichenvorrat der zu sichernden Kette.

Tabelle 2. **Gemischte Verfahren**

Bezeichnung ¹⁾ des Prüfzeichenverfahrens	Anwendung	Anzahl und Art der Prüfzeichen
ISO 7064, MOD 11, 10 ISO 7064, MOD 27, 26 ISO 7064, MOD 37, 36	Ziffernketten Buchstabenketten alphanumerische Ketten	1 Ziffer 1 Buchstabe 1 Ziffer oder Buchstabe
¹⁾ Die beiden Zahlen hinter ‚MOD‘ sind die beiden Moduln.		

4 Normkonformität und Produktbezeichnung

4.1 Zeichenketten

Eine Zeichenkette ist normgerecht, wenn sie mit einem Prüfzeichen versehen ist, das einem in dieser Norm für die betreffende Anwendung festgelegten Verfahren entspricht.

4.2 Produkte zur Erzeugung von Prüfzeichen

4.2.1 Produkte (Software oder Hardware), die ohne nähere Angabe als Prüfzeichen-erzeugend nach dieser Norm bezeichnet sind, müssen die Prüfzeichen für alle Verfahren dieser Norm erzeugen können.