Modulo – Teilen mit Rest

M1

Aufgabe:

Modulo ist eine Rechenoperation (wie z.B. Addition oder Multiplikation). Sie wird für zahlreiche Verschlüsselungsverfahren und auch für Schlüsselaustausch-Verfahren benötigt. Mit Modulo, **mod**, wird der Rest der ganzzahligen Division bezeichnet.

Beantworte die Fragen am Ende des Textes möglichst genau.

Zeit: 20‘ **Sozialform:** EA

Die Division mit Rest (Modulo) wird in der Programmierung relativ häufig verwendet. Der entsprechende Operator heisst in unterschiedlichen Programmiersprachen oft **mod** oder **%**. Man kann etwa prüfen, ob eine gegebene Zahlgerade ist, indem man folgende Abfrage durchführt:

```
if ((x mod 2) == 0)
```

Modulo kann man auch nutzen, wenn man in einer Schleife lediglich bei jedem -ten Schleifendurchlauf einen speziellen Programmcode ausführen will. Auch bei vielen Berechnungen und Algorithmen ist der Operator sinnvoll einsetzbar. Allgemein kann man mit **mod** prüfen, ob eine Zahl durch eine andere genau teilbar ist: Nur dann liefert der Modulo-Operator den Wert 0.

Bei der Modulo-Operation muss etwas gerechnet werden. Sie ist aber leicht zu verstehen.

Beispiel

Jeder von uns benutzt fast täglich die Modulo-Rechnung. Die kommt nämlich bei der Berechnung der Uhrzeit vor. Wir sagen zu der Uhrzeit 15:00 Uhr meist 3 Uhr (nachmittags). Das ist die Modulo-Rechnung mit der Zahl 12: 15 mod 12 = 3, da 15 : 12 = 1, 3 bleibt übrig.

Natürlich rechnet man nicht immer mod 12. 12 kann durch jede ganze Zahl ersetzt werden. Bei den meisten Verschlüsselungsverfahren kommen keine negativen Zahlen vor, das macht es etwas einfacher.

Beispielrechnungen

18 mod 5 = 3 , da 18 : 5 = 3 (Rest 3)
10 mod 4 = 2 , da 10 : 4 = 2 (Rest 2)
14 mod 7 = 0 , da 14 : 7 = 2 (Rest 0)

Weitere Beispiele aus der Informatik für die Anwendung von Modulo-Operationen.

- Berechnung der Prüfziffer der Internationalen Standardbuchnummer
- Prüfsummen-Formel Luhn-Algorithmus zur Bestätigung von Identifikationsnummern wie Kreditkartennummern und kanadische Sozialversicherungsnummern
- Kalenderberechnung (die relativ komplizierte Berechnung des Osterdatums)
- Berechnung der Prüfsumme der Internationalen Bankkontonummer (IBAN)
- In der Kryptografie, beim **Diffie-Hellman-Schlüsselaustausch** oder beim RSA-Kryptosystem.

Auftrag

1. Löse folgende Aufgaben:

25	*mod*	7	=		, da	25	:	7	=		, **Rest**	
90	*mod*	11	=		, da	90	:	11	=		, **Rest**	
23	*mod*	8	=		, da	23	:	8	=		, **Rest**	
10	*mod*	19	=		, da	10	:	19	=		, **Rest**	
106	*mod*	21	=		, da	106	:	21	=		, **Rest**	
42	*mod*	4	=		, da	42	:	4	=		, **Rest**	
8	*mod*	3	=		, da	8	:	3	=		, **Rest**	
33	*mod*	15	=		, da		:		=		, **Rest**	
107	*mod*	25	=		, da		:		=		, **Rest**	
2180	*mod*	54	=		, da		:		=		, **Rest**	
1011	*mod*	12	=		, da		:		=		, **Rest**	
1001	*mod*	13	=		, da		:		=		, **Rest**	
45	*mod*	14	=		, da		:		=		, **Rest**	
785	*mod*	43	=		, da		:		=		, **Rest**	

2. Löse folgende Aufgaben mit Hilfe von Python:

45´753	mod	17	=_____	4´257	mod	5	=_____
1089	mod	42	=_____	44´856	mod	78	=_____
407	mod	3	=_____	102´501	mod	20	=_____
186´023	mod	4´752	=_____	1´001	mod	14	=_____
412	mod	4	=_____	1´420	mod	04	=_____
1´040´445	mod	75´421	=_____	1´427´058	mod	45	=_____

Aufgabe für echte Hacker!°

Erstelle ein Programm in Python, welches die beiden Zahlen abfragt und daraus den Rest nach Division (Modulo) berechnet.

Bild Python IDLE mit Hinweisen zur Wiederholung