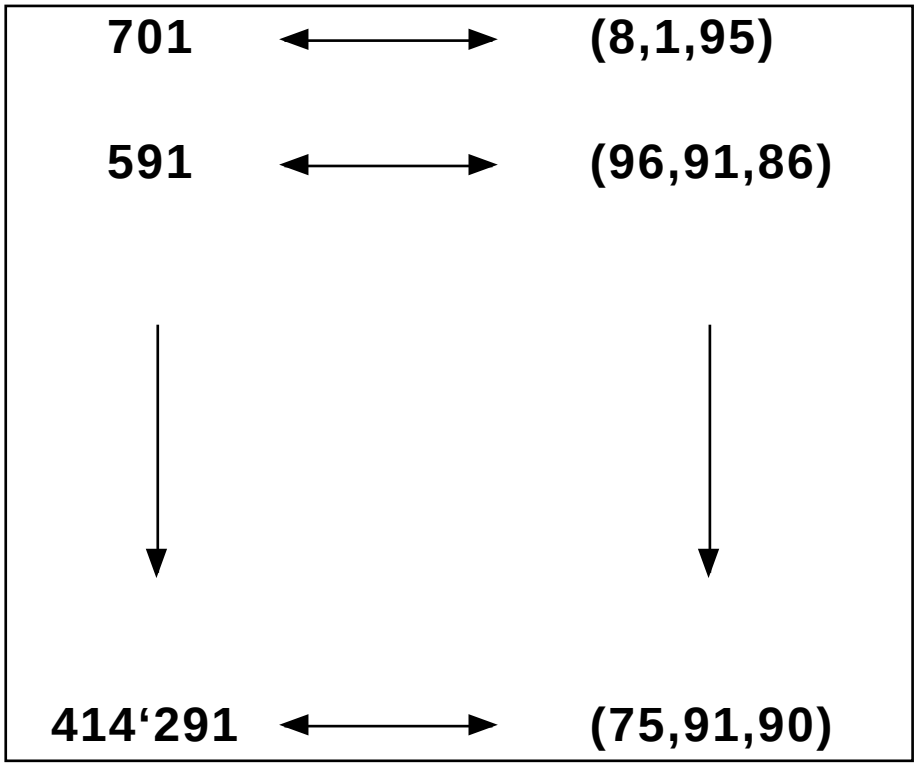
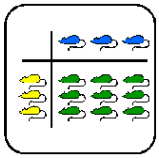
Modular-Multiplikation





Thema: Die Multiplikation mittels Modulo-Arithmetik
Schultyp: Mittelschule, Fachhochschule
Vorkenntnisse: Grundkenntnisse der Programmierung, Begriff des Parallelrechners, die Modulo-Funktion, chinesischer Restsatz aus der Zahlentheorie
Bearbeitungsdauer: 45 - 60 Minuten
Fassung vom: 15.9.95
Schulerprobung: nein

Übersicht

Der Posten erklärt ein konkretes Verfahren, das die schnelle Durchführung von Multiplikationen mittels Modulo-Arithmetik erlaubt. Die Schülerinnen und Schüler studieren zuerst die Theorie. Dann lösen sie ein einfaches Beispiel auf dem Papier. Schliesslich implementieren sie eine Funktion, welche die Multiplikation mittels Modulo-Arithmetik am Beispiel von 3 Moduli durchführt.

Lernziele

Nach Bearbeiten des Postens kennen die Schülerinnen und Schüler ein konkretes Verfahren, um zwei Zahlen mittels Modulo-Arithmetik multiplizieren zu können. Sie können das Verfahren an einfachen Beispielen selbst anwenden. Sie können diese Methode auch implementieren.

Material

- *Theorie*: Die Multiplikation mittels Modulo-Arithmetik

Quellen

Jurg Nievergelt: *Algorithms & Data Structures* - With Applications to Graphics and geometry. New Jersey 1993 (Prentice-Hall)

Hinweise, Lösungen

Lösung Auftrag 2

r = 000789
r mod 99 = 96
r mod 100 = 89
r mod 101 = 82

s = 000456
s mod 99 = 60
s mod 100 = 56
s mod 101 = 52

r * s ≈ (96, 89, 82) * (60, 56, 52) = (18, 84, 22)

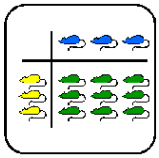
Lösung Auftrag 3

Nachfolgend ist die Funktion ModMult(a,b) als Beispiel mit den Moduli 99, 100, 101 in der Programmiersprache C implementiert:

```
void ModMult(a, b)
{
  int i,l;
  int r[3], s[3], rs[3];

  for (i=0; i<3; i++)
    {
      r[i] = a % (99 + i);
      s[i] = b % (99 + i);
    }

  for (i=0; i<3; i++)
    {
      rs[i] = (r[i] * s[i]) % (99 + i);
    }

  for (i=0; i<3; i++)
    {
      printf("%d * %d = [%d,%d,%d]\n",
             a, b, rs[0], rs[1], rs[2]);
    }
  l = 999900 - (494900*rs[0] + 9999*rs[1] + 495000*90) % 999900;
  printf("%d * %d = %d\n", a, b, l);
}
```

Hinweis zur Rücktransformation:
Die Richtigkeit der angegebenen Rücktransformationsformel ersieht man aus folgenden Berechnungen:

```
rs mod99 =  (-494900*rs[0]-9999*rs[1]-495000*90)%99
         = (-(99*4999-1)rs[0]-99*101*rs[1]-99*100*50*rs[2])%99
         = rs[0]
rs mod100 =(-100*101*49*rs[0]-(100*100-1)*rs[1]-100*99*50*rs[2])%100
          = rs[1]
rs mod101 =(-101*100*49*rs[0]-101*99*rs[1]-(101*49001-1)*rs[2])%101
          = rs[2]
```



Lehrer-Lernkontrolle / Test

Aufgabe 1

Du kennst die Multiplikation von zwei Zahlen mittels Modulo-Arithmetik. Löse damit folgende Rechnung: **987 x 654 = ?** Notiere die *einzelnen Schritte*, welche zum Resultat führen. Die Aufgabe ist dann gut gelöst, wenn aus den einzelnen Schritten ersichtlich ist, wie das Verfahren funktioniert. Der *Weg* ist wichtiger als das Resultat!

Aufgabe 2

Vergleiche die Berechnungskomplexität der modularen Multiplikation mit dejenigen der normalen Multiplikation.

Lösungen und Taxierung

Aufgabe 1

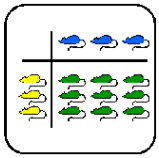
r = 000987
r mod 99 = 96
r mod 100 = 87
r mod 101 = 78

s = 000654
s mod 99 = 60
s mod 100 = 54
s mod 101 = 48

r * s ≈ (96, 87, 78) * (60, 54, 48) = (18, 98, 7)
Die Aufgabe verlangt vom Schüler eine Anpassung des Gelernten an eine leicht geänderte Problemstellung. Die Aufgabe ist deshalb als mindestens **K2** zu taxieren.

Aufgabe 2

Die Berechnungskomplexität der Schulmethode beträgt O(n*n), diejenige der modularen Multiplikation beträgt O(n).
Um die Aufgabe zu lösen, muss die Schülerin wiederum Teile des Gelernten abändern und auf eine neue Situation anwenden. Die Aufgabe ist deshalb als mindestens **K3** zu taxieren..



Werkstatt Multiplikation Auftragsblatt
Posten: **Modulare Multiplikation**

Was soll ich hier tun?

Du kennst die Schulmethode, zwei Zahlen miteinander zu multiplizieren.
Hier lernst Du ein neues Verfahren kennenlernen, das es erlaubt, zwei Zahlen miteinander zu multiplizieren Dieses Verfahren basiert auf der modularen Arithmetik. Der Posten besteht aus den folgenden drei Aufträgen:

(1) Studiere die **Theorie** "*Die Multiplikation mittels Modular-Arithmetik*" (20 - 30 Minuten)
(2) Löse folgende Multiplikation **789 x 456 = ?** Verwende die modulare Arithmetik zur Berechnung des Resultats. (5 Minuten)
(3) Implementiere eine Funktion in der von Dir verwendeten Programmiersprache, welche das Produkt von zwei Zahlen zwischen 0 und 999 mittels Modulo-Arithmetik berechnet.(10 - 15 Minuten)

Den Theorieteil sollte jeder für sich studieren. Die Aufträge (2) und (3) könnt Ihr, wenn Ihr wollt, auch in Gruppen (2 oder 3 Personen) bearbeiten.

Die Multiplikation mittels Modular-Arithmetik

Das Ziel der Multiplikation mittels Modular-Arithmetik ist es, die Multiplikation zweier grosser Zahlen in mehrere Multiplikaionen von kleineren Zahlen zu zerlegen. Dies ist vorallem im Bereich der Programmierung von Vorteil. Einerseits erlaubt ein solches Verfahren die Multiplikation von Zahlen ausserhalb des Darstellungsbereichs des Computers, andererseits können die "kleineren" Multiplikationen sehr effizient parallel auf den Computer durchgeführt werden.
Die Theorie für diese spezielle Art der Multiplikation beruht auf dem sogenannten chinesischen Restsatz. Zur Erinnerung hier die Version des chinesischen Restsatzes für drei Moduli.
Chinesischer Restsatz: Falls für drei Zahlen m1, m2 und m3 gilt, dass das kleinste gemeinsame Vielfache die Zahl m1 x m2 x m3 ist, kann jede ganze Zahl u zwischen 0 und (m1 x m2 x m3 -1) eindeutig als Tripel (u mod m1, u mod m2, u mod m3) dargestellt werden.

Als Beispiel: Wir betrachten die drei Zahlen 99, 100, und 101. Das kleinste gemeinsame Vielfache ist 999'900 (= 99 x 100 x 101). Die Zahl 414291 wird auf das Tripel (75, 91, 90) abgebildet. Keine andere Zahl zwischen 0 und 999'899 wird auf das Tripel (75, 91, 90) abgebildet. Das heisst, dass wir aus dem Tripel (75, 91, 90) wieder die Zahl 414291 rekonstruieren können.
Wollen wir nun zwei Zahlen zwischen 0 und 999'899 miteinander multiplizieren, können wir diese Zahlen zuerst auf das entsprechende Tripel abbilden und danach die einzelnen Zahlen miteinander multiplizieren.

Als Beispiel: Wir wollen 701 und 591 multiplizieren. Diesen beiden Zahlen entsprechen den Tripeln (8, 1, 95) und (96, 91, 86). Das Resultat (701 x 591 =) 414291 entspricht dem Tripel (75, 91 90). Wir müssen nun aber nicht die ursprünglichen Zahlen 701 und 591 miteinander multiplizieren, sondern können direkt die Tripel miteinander multiplizieren. Wir rechnen also (8 x 96) mod 99 = 75; (1 x 91) mod 100 = 91 und (95 x 86) mod 99 = 90. So erhalten wir direkt das Tripel (75, 91, 90). Mit der hier nicht weiter erlaüterten Rück-transformationsformel:

(-494900 x 75 - 9999 x 91 - 495000 x 90) mod 999900

erhalten wir 414291. Dies entspricht wie erwartet 701 x 591.

Zusammenfassung: