

# Einführung in die Zahlentheorie 1 - Übung


Prof. Dr. Josef F. Bürgler

I.BA\_DMATH, Semesterwoche 9

Die Aufgaben sind zusammen mit dem Lösungsweg in möglichst einfacher Form darzustellen. Numerische Resultate sind mit einer Genauigkeit von 4 Stellen anzugeben. Skizzen müssen qualitativ und quantitativ richtig sein.

Sie sollten im Durchschnitt 75% der Aufgaben bearbeiten. Die mit grossen römischen Zahlen gekennzeichneten Aufgaben **müssen** bearbeitet werden und die Lösungen dieser Aufgaben werden kontrolliert und bewertet. Abgabetermin ihrer Übungsaufgaben ist die letzte Vorlesungsstunde in der Woche, nachdem das Thema im Unterricht besprochen wurde.

Referenz: *Kenneth H. Rosen, Discrete Mathematics and its Applications, McGraw-Hill International Edition, 6. Auflage, kurz: KR*

1. **KR, Abschnitt 3.4, Aufgabe 17:** Berechnen Sie die folgenden Ausdrücke:  $13 \bmod 3$ ,  $-97 \bmod 11$ ,  $155 \bmod 19$  und  $-221 \bmod 23$ .
2. **KR, Abschnitt 3.4, Aufgabe 19:** Entscheiden Sie, welche der folgenden Zahlen kongruent zu 5 modulo 17 sind: 80, 103,  $-29$  und  $-122$ .
3. Sei  $n$  eine natürliche Zahl mit  $n \geq 2$ . Bestimmen Sie die folgenden Ausdrücke. Sie können das Ergebnis natürlich erraten, wenn Sie einige  $n$  ausprobieren. Geben Sie dann aber eine nachvollziehbare allgemeine (für alle  $n \geq 2$  gültige) Begründung für Ihr Ergebnis.
  - a)  $(n+2) \bmod (n+1)$ ,
  - b)  $(2n+2) \bmod (n+1)$ ,
  - c)  $(n^2+1) \bmod (n+1)$ ,
  - d)  $n^2 \bmod (n+1)$ ,
  - e)  $(n+1)^2 \bmod n$ ,
  - f)  $(n+1)^{1000} \bmod n$ ,
  - g)  $(n-1)^2 \bmod n$ .
-  4. Sei  $n$  eine natürliche Zahl mit  $n \geq 2$ . Bestimmen Sie die folgenden Ausdrücke. Sie können das Ergebnis natürlich erraten, wenn Sie einige  $n$  ausprobieren. Geben Sie dann aber eine nachvollziehbare allgemeine (für alle  $n \geq 2$  gültige) Begründung für Ihr Ergebnis.
  - a)  $(n+1) \bmod n$ ,
  - b)  $n^2 \bmod n$ ,

- c)  $(3n+6) \bmod n$ ,
- d)  $(4n-1) \bmod n$ ,
- e)  $((n+1)n) \bmod n$ ,
- f)  $(n^3+2n^2+4) \bmod n$ ,
- g)  $((2n+2)(n+1)) \bmod n$  und
- h)  $n! \bmod n$ .

4. **KR, Abschnitt 3.6, Aufgabe 23:** Bestimmen Sie mit dem Euklidischen Algorithmus

- a)  $\text{ggT}(12, 18)$ ,
- b)  $\text{ggT}(111, 201)$  und
- c)  $\text{ggT}(1001, 1331)$ .

II. Bestimmen Sie mit dem Euklidischen Algorithmus Schritt für Schritt  $\text{ggT}(587, 392)$ . Bestimmen Sie dann ebenfalls von Hand eine Zahl  $x$  ( $0 \leq x \leq 587$ ) so, dass gilt:  $392 \cdot x \equiv (1 \bmod 587)$ .

5. a) Bestimmen Sie **Schritt für Schritt und per Hand** eine ganzzahlige Lösung  $(x, y)$  der diophantischen Gleichung

$$144 \cdot x + 37 \cdot y = 1.$$

- b) Bestimmen Sie zwei **natürliche** Zahlen  $a_1$  und  $a_2$ , so dass Folgendes gilt:

$$144 \cdot a_1 \equiv 1 \pmod{37} \quad \text{und} \quad 37 \cdot a_2 \equiv 1 \pmod{144}.$$

III. **KR, Abschnitt 3.7, Aufgabe 19:** Bestimmen Sie alle Lösungen des Systems von linearen Kongruenzen:

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{11} \end{aligned}$$

6. **KR, Abschnitt 3.7, Aufgabe 27:**

- a) Beweisen Sie mit Hilfe des kleinen Satzes von Fermat, dass  $2^{340} \equiv 1 \pmod{11}$  gilt. (Hinweis:  $2^{340} = (2^{10})^{34}$ )
  - b) Beweisen Sie, dass  $2^{340} \equiv 1 \pmod{31}$  gilt. (Hinweis:  $2^{340} = (2^5)^{68} = 32^{68}$ )
  - c) Nutzen Sie die beiden obigen Resultate, um zu zeigen dass,  $2^{340} \equiv 1 \pmod{341}$  gilt.
7. Berechnen Sie  $\phi(6)$ ,  $\phi(11)$  und  $\phi(13)$ , indem Sie jeweils die Menge  $\mathbb{Z}_n$  für  $n = 6$ ,  $n = 11$  und  $n = 13$  aufschreiben. Verifizieren Sie anhand dieser Beispiele, dass  $\phi(p) = p - 1$  falls  $p$  eine Primzahl ist!

IV. Rechnen Sie **nicht**  $12!$  aus, sondern faktorisieren  $12!$  und verwenden Sie dann den Satz auf den Folien um die  $\phi$ -Funktion einer zusammengesetzten Zahl zu berechnen.

8. Bestimmen Sie die ungefähre Anzahl der Primzahlen mit 512 Bit. Hinweis: Schätzen Sie den Wert  $\pi(2^{513}) - \pi(2^{512})$ .

9. a) Berechnen Sie die Binomialkoeffizienten  $\binom{5}{1}$ ,  $\binom{5}{2}$ ,  $\binom{5}{3}$  und  $\binom{5}{4}$  (per Hand) und zeigen Sie, dass diese durch 5 teilbar sind.

- b) Sei  $p$  eine Primzahl. Zeigen (bzw. begründen) Sie, dass die Binomialkoeffizienten

$$\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$$

durch  $p$  teilbar sind

## Lösungen

1. 1, 2, 3 und 9
2. nein, nein, ja, nein
3. a)  $(n+2) \bmod (n+1) = 1$ , denn  $(n+2) = 1 \cdot (n+1) + 1$   
b)  $(2n+2) \bmod (n+1) = 0$ , denn  $(2n+2) = 2 \cdot (n+1) + 0$   
c)  $(n^2+1) \bmod (n+1) = 2$ , denn  $(n^2+1) = (n-1) \cdot (n+1) + 2$  (binomische Formel)  
d)  $n^2 \bmod (n+1) = 1$ , denn  $n^2 = (n-1) \cdot (n+1) + 1$  (binomische Formel)  
e)  $(n+1)^2 \bmod n = 1$ , denn  $(n+1)^2 = (n+2) \cdot n + 1$   
f)  $(n+1)^{1000} \bmod n = 1$ , denn mit Hilfe des binomischen Lehrsatzes gilt:

$$\begin{aligned}(n+1)^{1000} &= \sum_{k=0}^{1000} \binom{1000}{k} n^k \\&= \binom{1000}{0} n^0 + \binom{1000}{1} n^1 + \binom{1000}{2} n^2 + \dots + \binom{1000}{1000} n^{1000} \\&= 1 + \left( \binom{1000}{1} n^0 + \binom{1000}{2} n^1 + \dots + \binom{1000}{1000} n^{999} \right) \cdot n\end{aligned}$$

g)  $(n-1)^2 \bmod n = 1$ , denn  $(n-1)^2 = (n-2) \cdot n + 1$ .

I. -

4.  $\text{ggT}(12, 18) = 6$ ,  $\text{ggT}(111, 201) = 3$  und  $\text{ggT}(1001, 1331) = 11$

II. -

5. a)

$$144 \cdot 9 + 37 \cdot (-35) = 1.$$

b)

$$144 \cdot 9 \equiv 1 \pmod{37} \quad \text{und} \quad 37 \cdot 109 \equiv 1 \pmod{144}$$

III.  $x \equiv \underbrace{(1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot (-1) + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot (-4))}_{=-337} \pmod{330}$

6.

7.

IV. Wegen  $12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$  hat man mit Hilfe der Rechenregel für die  $\phi$ -Funktion einer zusammengesetzten Zahl

$$\phi(12!) = \phi(2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11) = 1 \cdot 2^9 \cdot 2 \cdot 3^4 \cdot 4 \cdot 5^1 \cdot 6 \cdot 10 = 2^{13} \cdot 3^4 \cdot 5^2 \cdot 6 = 99'532'800.$$

8.  $\pi(2^{513}) - \pi(2^{512}) \approx 2^{503}$  (Primzahlsatz)

9. a) Direkte Rechnung: 5, 10, 10, 5

b) Hinweis:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1) \cdots (p-k+1)}{1 \cdot 2 \cdots k}$$

$$\text{I. a) } n \bmod n = 0 \\ 1 \bmod n = 1 \rightarrow \underline{1}$$

$$\text{b) } n^2 \bmod n = n \bmod n = \underline{0}$$

$$\text{vgl. } m^p \bmod p = m \bmod p$$

$$\text{c) } 3n + 6 \bmod n = \overbrace{3n \bmod n}^{=0} + 6 \bmod n = 6 \bmod n = \underline{6}$$

$$\text{d) } 4n - 1 \bmod n = 4n \bmod n - 1 \bmod n = -1 \bmod n = \underline{-1}$$

$$\text{e) } (n+1)n \bmod n = (n+1) \bmod n \cdot n \bmod n = 1 \cdot 0 = \underline{0}$$

$$\text{f) } n^3 + 2n^2 + 4 \bmod n = n \bmod n + 2n \bmod n + 4 \bmod n = \underline{4}$$

$$\text{g) } (2n+2)(n+1) \bmod n = 2 \bmod n \cdot 1 \bmod n = \underline{2}$$

$$\text{h) } n! \bmod n = \underbrace{n \bmod n}_{=0} \cdot (n-1) \bmod n \cdot \dots = \underline{0}$$

$$\text{II. } \text{ggT}(587, 392)$$

$$587 = 1 \cdot 392 + 195$$

$$392 = 2 \cdot 195 + 2$$

$$195 = 97 \cdot 2 + \underline{1} - \text{ggT}$$

$$2 = 2 \cdot 1 + 0$$

erweiterter Algorithmus

$$1 = 195 - 97 \cdot 2$$

$$1 = 195 - 97 \cdot (392 - 2 \cdot 195)$$

$$= 195 - 97 \cdot 392 + 194 \cdot 195$$

$$= 195 \cdot 195 - 97 \cdot 392$$

$$= 195 \cdot (587 - 392) - 97 \cdot 392$$

$$= \underline{\underline{195 \cdot 587 - 292 \cdot 392}}$$

$$195 \cdot 587 - 292 \cdot 392 \equiv 1 \pmod{587}$$

$$(195 \cdot 587 - 292 \cdot 392) \pmod{587} = 1 \pmod{587}$$

$$195 \cdot 587 \pmod{587} - 292 \cdot 392 \pmod{587} = 1 \pmod{587}$$

$$0 - 292 \cdot 392 \pmod{587} = 1 \pmod{587}$$

$$\Rightarrow \underline{\underline{392 \cdot 292 \equiv 1 \pmod{587}}}$$

$$\text{III. } x = \sum_{i=1}^k r_i \cdot M_i \cdot y_i$$

$$m = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

$$M_1 = \frac{m}{2} = 165$$

$$M_2 = \frac{m}{3} = 110$$

$$M_3 = \frac{m}{5} = 66$$

$$M_4 = \frac{m}{11} = 30$$

$$165 \cdot y_1 = 1 \pmod{2}$$

$$165 = 82 \cdot 2 + 1$$

$$1 = 165 - 82 \cdot 2 \Rightarrow ax - q \cdot m = 1 \quad y_1 = \underline{\underline{1}}$$

$$110 \cdot y_2 = 1 \pmod{3}$$

$$110 y_2 + 3x = 1$$

$$110 = 36 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$1 = 3 - 2$$

$$= 3 - 1(110 - 36 \cdot 3)$$

$$= 3 \cdot 110 + 36 \cdot 3$$

$$1 = -110 + 37 \cdot 3$$

$$y_2 = -1 \equiv 2 \pmod{3} = \underline{\underline{2}}$$

+3 Abstand vielfaches von 3

$$66 \cdot y_3 = 1 \pmod{5}$$

$$66y_3 + 5x = 1$$

$$66 = 13 \cdot 5 + 1 \Rightarrow 1 = 66 - 13 \cdot 5$$

$$y_3 = \underline{\underline{1}}$$

$$30y_4 = 1 \pmod{11}$$

$$30y_4 + 11x = 1$$

$$30 = 2 \cdot 11 + 8 \Rightarrow 3 \cdot 11 - 4(30 - 2 \cdot 11) = 3 \cdot 11 - 4 \cdot 30 + 8 \cdot 11$$

$$11 = 1 \cdot 8 + 3 \qquad \qquad \qquad = 11 \cdot 11 - 4 \cdot 30$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$y_4 = -4 \equiv 7 \pmod{11} = \underline{\underline{7}}$$

+11

$$x = \sum_{i=1}^k r_i \cdot M_i \cdot y_i \quad ; \quad r_1=1, r_2=2, r_3=3, r_4=4$$

$$\rightarrow 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7 = 1643$$

$$= 1643 \pmod{330}$$

$$= \underline{\underline{323 \pmod{330}}}$$



$$\begin{aligned}\text{IV. } \phi(12!) &= \phi(2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11) \\ &= 1 \cdot 2^9 \cdot 2 \cdot 3^4 \cdot 4 \cdot 5^1 \cdot 6 \cdot 10 \\ &= 2^{13} \cdot 3^4 \cdot 5^2 \cdot 6 \\ &= \underline{\underline{99'532'800}}\end{aligned}$$