Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

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: $13 \textbf{ mod } 3$, $-97 \textbf{ mod } 11$, $155 \textbf{ mod } 19$ und $-221 \textbf{ mod } 23$.
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) $(n+2) \textbf{ mod } (n+1)$,
   b) $(2n+2) \textbf{ mod } (n+1)$,
   c) $(n^2+1) \textbf{ mod } (n+1)$,
   d) $n^2 \textbf{ mod } (n+1)$,
   e) $(n+1)^2 \textbf{ mod } n$,
   f) $(n+1)^{1000} \textbf{ mod } n$,
   g) $(n-1)^2 \textbf{ mod } n$.

I. 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) $(n+1) \textbf{ mod } n$,
   b) $n^2 \textbf{ mod } n$,

c) $(3n+6) \ \mathbf{mod}\ n$,

d) $(4n-1) \ \mathbf{mod}\ n$,

e) $((n+1)n) \ \mathbf{mod}\ n$,

f) $(n^3+2n^2+4) \ \mathbf{mod}\ n$,

g) $((2n+2)(n+1)) \ \mathbf{mod}\ n$ und

h) $n! \ \mathbf{mod}\ n$.

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

   a) $\mathrm{ggT}(12, 18)$,

   b) $\mathrm{ggT}(111, 201)$ und

   c) $\mathrm{ggT}(1001, 1331)$.

II. Bestimmen Sie mit dem Euklidschen Algorithmus Schritt für Schritt 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 ϕ-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

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

durch p teilbar sind

Lösungen

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

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

   g) $(n-1)^2\ \mathbf{mod}\ n = 1$, denn $(n-1)^2 = (n-2)\cdot n+1$.

I. -

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

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 ϕ-Funktion einer zusammengesetzten Zahl

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

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

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

   b) Hinweis:

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