Probeklausur zur Vorlesung Angewandte Diskrete Mathematik

Institut für Reine Mathematik WS 08/09

Freitag, 05.12.2008, 14.15 – 16.oo

Es gibt auf dieser Klausur 15 Teilaufgaben. Jede Teilaufgabe wird mit 4 Punkten bewertet. Damit sind insgesamt 60 Punkte zu erreichen.

1. (a) Zeigen Sie: Die Zahlen 457 , 359 sind teilerfremd.
Lösung: Wir verwenden den Euklidischen Algorithmus:

$$\begin{aligned} 457 &= 1 \cdot 359 + 98 \\ 359 &= 3 \cdot 98 + 65 \\ 98 &= 1 \cdot 65 + 33 \\ 65 &= 1 \cdot 33 + 32 \\ 33 &= 1 \cdot 32 + 1 \end{aligned}$$

Damit gilt $\mathrm{ggT}(457, 359) = 1$.

(b) Bestimmen Sie das multiplikative Inverse von 359 modulo 457 .
Lösung: Aus der Lösung für (a) gewinnen wir eine Darstellung $1 = a \cdot 359 + b \cdot 457$ wie folgt:

$$\begin{aligned} 1 &= 33 - 32 \\ &= 33 - (65 - 33) \\ &= 2 \cdot 33 - 65 \\ &= 2 \cdot (98 - 65) - 65 \\ &= 2 \cdot 98 - 3 \cdot 65 \\ &= 2 \cdot 98 - 3 \cdot (359 - 3 \cdot 98) \\ &= 11 \cdot 98 - 3 \cdot 359 \\ &= 11 \cdot (457 - 359) - 3 \cdot 359 = 11 \cdot 457 - 14 \cdot 359. \end{aligned}$$

Damit ist das Multiplikative Inverse zu 359 gerade $-14 \equiv 443 \mod 457$.

2. (a) Was besagt der Satz von Euler?
Lösung: Sind a, m *teilerfremd*, so gilt $a^{\varphi(m)} \equiv 1 \mod m$.

(b) Berechnen Sie $5^{99} \mod 104$.
Lösung: Es sind $5, 104$ teilerfremd, daher können wir den Satz von Euler anwenden. Es ist $104 = 8 \cdot 13$, damit gilt $\varphi(104) = 4 \cdot 12 = 48$. Wegen $99 = 2 \cdot 48 + 3$ folgt daher

$$5^{99} \equiv 5^{2 \cdot 48 + 3} \equiv 5^3 \equiv 125 \equiv 21 \mod 104.$$

(c) Berechnen Sie die letzten zwei Stellen von 2^{80} .
Lösung: Gesucht ist also $2^{80} \mod 100$. Die Zahlen $2, 100$ sind *nicht* teilerfremd, daher können wir den Satz von Euler so nicht anwenden. Wir bestimmen daher zunächst $2^{80} \mod 25$. Hier können wir den Satz von Euler anwenden; es gilt $\varphi(25) = 4 \cdot 5 = 20$. Daher gilt $2^{80} \equiv 1 \mod 25$. Damit gilt $2^{80} \equiv 1, 26, 51$ oder $76 \mod 100$. Da 4 ein Teiler von 2^{80} ist, gilt $2^{80} \equiv 0 \mod 4$, und damit folgt $2^{80} \equiv 76 \mod 100$. Die letzten zwei Stellen sind also 76 .

3. (a) Es seien a, m teilerfremd. Wie ist der Exponent von a modulo m definiert?
Lösung: Der Exponent ist die *kleinste positive* Zahl e mit $a^e \equiv 1 \mod m$.

(b) Bestimmen Sie den Exponenten von 6 modulo 49 .
Lösung: Es ist $\varphi(49) = 6 \cdot 7 = 42$. Da der Exponent immer ein Teiler von $\varphi(m)$ ist, sind die

möglichen Exponenten $1, 2, 3, 6, 7, 14, 21, 42$. Es ist

$$\begin{aligned} 6^2 &\equiv 36 \mod 49 \\ 6^3 &\equiv 216 \equiv 20 \mod 49 \\ 6^6 &\equiv 20^2 \equiv 400 \equiv 8 \mod 49 \\ 6^7 &\equiv 6 \cdot 8 \equiv 48 \equiv -1 \mod 49 \\ 6^{14} &\equiv (-1)^2 \equiv 1 \mod 49 \end{aligned}$$

Damit ist der Exponent gerade 14

(c) Ist 6 eine Primitivwurzel modulo 49 ? Begründen Sie Ihre Antwort.

Lösung: a ist Primitivwurzel modulo m genau dann, wenn der Exponent gerade $\varphi(m)$ ist. Da der Exponent von 6 aber $14 < \varphi(49) = 42$ ist, ist 6 keine Primitivwurzel modulo 49 .

4. Bestimmen Sie alle Quadratwurzeln von 58 modulo 77 .

Lösung: Es ist $77 = 7 \cdot 11$. Wir bestimmen zunächst die Wurzeln modulo 7 , 11 getrennt und fügen sie dann mit dem Chinesischen Restsatz zusammen. Es ist $58 \equiv 2 \mod 7$, $58 \equiv 3 \mod 11$. Die Wurzel aus 2 modulo 7 bekommen wir über $2^{(7+1)/4} = 2^2 = 4$, da $7 \equiv 3 \mod 4$. Zur Kontrolle: $4^2 = 16 \equiv 2 \mod 7$. Damit sind die Wurzeln aus 2 modulo 7 gerade $\pm 4 \equiv \mp 3$.
Die Wurzel aus 3 modulo 11 bekommen wir analog über $3^{(11+1)/4)} = 3^3 = 27 \equiv 5 \mod 11$. Damit sind die Wurzeln aus 3 modulo 11 gerade ± 5 . Zur Kontrolle: $5^2 = 25 \equiv 3 \mod 11$.
Die Zahlen $7, 11$ sind teilerfremd mit $1 = 2 \cdot 11 - 3 \cdot 7$ (direkt, oder per Erweitertem Euklidischem Algorithmus). Damit bekommen wir die Wurzeln über den Chinesischen Restsatz wie folgt:

$$\begin{aligned} &x_1 \equiv 3 \mod 7, \quad x_1 \equiv 5 \mod 11 \Longrightarrow x_1 \equiv 3 \cdot 22 - 5 \cdot 21 \equiv 66 - 105 \equiv -39 \equiv 38 \mod 77, \\ &x_2 \equiv -3 \mod 7, \quad x_2 \equiv 5 \mod 11 \Longrightarrow x_2 \equiv -3 \cdot 22 - 5 \cdot 21 \equiv -66 - 105 \equiv -171 \equiv 60 \mod 77, \\ &x_3 \equiv 3 \mod 7, \quad x_3 \equiv -5 \mod 11 \Longrightarrow x_3 \equiv -x_2 \equiv -60 \equiv 17 \mod 77, \\ &x_4 \equiv -3 \mod 7, x_4 \equiv -5 \mod 11 \Longrightarrow x_4 \equiv -x_1 \equiv -38 \equiv 39 \mod 77. \end{aligned}$$

5. Berechnen Sie $3^{41} \mod 79$.

Wir benutzen den Algorithmus zum schnellen Potenzieren. Dabei ist $41 = 32 + 8 + 1 = (101001)_2$.

$$\begin{aligned} & r := 1, a := 3 \\ i = 0: \quad & r := r \cdot a = 1 \cdot 3 = 3 \\ & a := a^2 = 9 \\ i = 1: \quad & r := 3 \\ & a := a^2 = 9^2 = 81 \equiv 2 \mod 79 \\ i = 2: \quad & r := 3 \\ & a := a^2 = 2^2 = 4 \\ i = 3: \quad & r := r \cdot a = 3 \cdot 4 = 12 \\ & a := a^2 = 4^2 = 16 \\ i = 4: \quad & r := 12 \\ & a := a^2 = 16^2 = 256 = 240 + 16 \equiv 3 + 16 = 19 \mod 79 \\ i = 5: \quad & r := r \cdot a = 12 \cdot 19 = 240 - 12 \equiv 3 - 12 = -9 \equiv 70 \mod 79 \end{aligned}$$

Es gilt also $3^{41} \equiv 70 \mod 79$.

6. Betrachten Sie das RSA-Verfahren mit $N = 85$ und $e = 5$.

(a) Wie lautet der geheime Schlüssel d ?

Lösung: d ist gerade das multiplikative Inverse von e modulo $\varphi(N)$. Es ist $N = 5 \cdot 17$, also $\varphi(N) = 4 \cdot 16 = 64$. Wir wenden den Erweiterten Euklidischen Algorithmus an:

$$\begin{aligned} 64 &= 12 \cdot 5 + 4 \\ 5 &= 4 + 1 \end{aligned}$$

Damit folgt $1 = 5 - 4 = 5 - (64 - 12 \cdot 5) = 13 \cdot 5 - 64$. Damit folgt $d = 13$.

(b) Verschlüsseln Sie die Nachricht 7 .

Lösung: Berechne $7^5 \mod 85$: $7^2 = 49$, $7^3 = 49 \cdot 7 = 343 \equiv 3 \mod 85$. Damit ist $7^5 = 7^2 \cdot 7^3 \equiv 49 \cdot 3 \equiv 147 \equiv 62 \mod 85$. Die verschlüsselte Nachricht lautet also: 62 .

(c) Entschlüsseln Sie die Nachricht 2 .

Lösung: Berechne $2^{13} \mod 85$. Es ist $2^7 = 128 \equiv 43 \mod 85$. Damit ist $2^8 \equiv 86 \equiv 1 \mod 85$. Daraus folgt dann $2^{13} \equiv 2^5 \equiv 32 \mod 85$. Die entschlüsselte Nachricht lautet also: 32 .

7. Neun Piraten haben einen Goldschatz gefunden, der aus weniger als 500 Münzen besteht. Als sie den Schatz gleichmäßig aufteilen wollen, bleibt eine Münze übrig. Da sie sich nicht entscheiden können, wem diese Münze gehören soll, geraten sie so heftig in Streit, dass einer von ihnen dabei umkommt. Als sie versuchen, den Schatz nun auf alle Überlebenden aufzuteilen, bleiben 2 Münzen übrig. Darüber geraten sie wieder in Streit, und wieder stirbt ein Pirat. Nun lässt sich der Goldschatz auf die übrigen Piraten gleichmäßig aufteilen. Wie viele Münzen haben die Piraten gefunden?

Lösung: Wir haben das folgende System von Kongruenzen zu lösen:

$$x \equiv 1 \mod 9, \quad x \equiv 2 \mod 8, \quad x \equiv 0 \mod 7.$$

Dazu benutzen wir den Chinesischen Restsatz. Dabei ist $M_1 = 8 \cdot 7 = 56$, $M_2 = 9 \cdot 7 = 63$, $M_3 = 9 \cdot 8 = 72$. Nun benötigen wir die Inversen von M_i modulo m_i .
Zunächst ist $M_1 = 56 \equiv 2 \mod 9$. Wegen $5 \cdot 2 = 10 \equiv 1 \mod 9$ ist daher $e_1 = 5$ das Inverse zu M_1 .
Weiter ist $M_2 = 63 \equiv 7 \equiv -1 \mod 8$. Daher ist $e_2 = -1 \equiv 7$ das Inverse zu M_2 .
Weiter ist $M_3 = 72 \equiv 2 \mod 7$. Wegen $4 \cdot 2 = 8 \equiv 1 \mod 7$ ist daher $e_3 = 4$ das Inverse zu M_3 .
Damit erhalten wir

$$\begin{aligned} x &\equiv 1 \cdot M_1 \cdot e_1 + 2 \cdot M_2 \cdot e_2 + 0 \cdot M_3 \cdot e_3 \\ &\equiv 1 \cdot 56 \cdot 5 + 2 \cdot 63 \cdot (-1) \\ &\equiv 280 - 126 \equiv 154. \end{aligned}$$

Die Piraten haben also 154 Goldmünzen gefunden.

8. Zeigen Sie: $11^n \equiv 10n + 1 \mod 100$ für alle $n \geqslant 1$.

Lösung: *Variante 1: Vollständige Induktion* Im Fall $n = 1$ ist $11^1 = 11 = 10 \cdot 1 + 1$. Damit ist die Behauptung richtig für $n = 1$. Im Induktionsschritt betrachte

$$11^{n+1} = 11 \cdot 11^n \equiv 11 \cdot (10n + 1) \equiv 110n + 11 \equiv 10n + 11 \equiv 10(n + 1) + 1.$$

Damit folgt die Behauptung.
Variante 2: Der binomische Lehrsatz Es gilt

$$11^n = (1 + 10)^n = 1 + n \cdot 10 + \binom{n}{2} \cdot 10^2 + \binom{n}{3} \cdot 10^3 + \cdots + 10^n.$$

Die hinteren Terme mit 10^k für $k \geqslant 2$ sind $\equiv 0 \mod 100$. Damit folgt $11^n \equiv 1 + n \cdot 10$ wie behauptet.