Musterlösung zur Probeklausur zur Angewandten Diskreten Mathematik

Dr. Hartmut Lanzinger, Hans- Peter Reck

Gesamtpunktzahl: 114 Punkte, 100 Punkte= 100 %, keine Abgabe

1. Es seien $m = 1155$ und $n = 1280$.

   (a) Bestimme die Primfaktorzerlegung von m und n.
   Es gilt
   $$m = 5 \cdot 231 = 5 \cdot 3 \cdot 77 = 3 \cdot 5 \cdot 7 \cdot 11$$
   sowie
   $$n = 10 \cdot 128 = 2 \cdot 5 \cdot 2^7 = 2^8 \cdot 5.$$

   (b) Leite daraus $ggT(m,n)$ und $kgV(m,n)$ als Produkt von Primfaktoren her.

   Beim größten gemeinsamen Teiler benötigen wir das Maximum der jeweils auftretenden Primfaktoren in m und n. Daher ergibt sich $ggT(m,n) = 5$. Analog ist das kleinste gemeinsame Vielfache durch die Primfaktoren definiert, die entweder in m oder in n auftreten. Daher ist $kgV(m,n) = 2^8 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. (7 Punkte)

2. Es seien $n, m \in \mathbb{N}$. Zeige: Ist 3 ein Teiler von $n^2 + m^2$, so teilt 3 bereits n und m.

   Da 3 ein Teiler von $m^2 + n^2$ ist, gilt $n^2 + m^2 \equiv 0 \bmod 3$.
   Wir zeigen die Aussage mit einem Beweis durch Widerspruch und nehmen es, es gelte OBDA $3 \nmid n$. Dann gilt $n \equiv \pm 1 \bmod 3$ und daraus folgt $n^2 \equiv 1 \bmod 3$. Folglich ist $n^2 + m^2 \equiv 1 + m^2 \equiv 0 \bmod 3$ nach Vorausetzung, woraus allerdings $m^2 \equiv 2 \bmod 3$ folgt. Dies ist aber nicht möglich, da für $m \equiv \pm 1 \bmod 3$ wie oben $m^2 \equiv 1 \bmod 3$ bzw. für $m \equiv 0 \bmod 3$ analogerweise $m^2 \equiv 0 \bmod 3$ folgt, ein Widerspruch. Also gilt $3|n$, und wegen $3|(n^2 + m^2)$ muss auch $3|m$ gelten. (5 Punkte)

3. (a) Bestimme den größten gemeinsamen Teiler von 6141 und 3243.

   Wir wenden den Euklidischen Algorithmus auf die beiden Zahlen an, nutzen dazu das Tabellenschema und bekommen

n	r_n	q_n	x_n	y_n
-1	6141	-	1	0
0	3243	-	0	1
1	2898	1	1	-1
2	345	1	-1	2
3	138	8	9	-17
4	69	2	-19	36
5	0	2		

   Also gilt $ggT(6141, 3243) = 69$.

(b) Ist die Diophantische Gleichung $6141x + 3243y = 207$ lösbar?
Falls ja, gib hierfür eine Lösung an.

Wegen $ggT(6141, 3243) = 69|207$ besitzt diese Diophantische Gleichung Lösungen. Dem Tabellenschema von Teilaufgabe a) entnehmen wir $ggT(6141, 3243) = 69 = -19 \cdot 6141 + 36 \cdot 3243$. Multiplikation dieser Gleichung mit 3 ergibt $-19 \cdot 3 \cdot 6141 + 36 \cdot 3 \cdot 3243 = 207$, also lösen $x = -57$ und $y = 108$ die gegebene Diophantische Gleichung. (10 Punkte)

4. (a) Gib alle Lösungen der linearen Kongruenz $23x \equiv 31 \bmod 47$ an.

Wir führen diese lineare Kongruenz auf eine Diophantische Gleichung zurück, und zwar auf die Gleichung $23x + 47y = 31$. Diese lösen wir erneut mit dem Tabellenschema. Es ist

n	r_n	q_n	x_n	y_n
-1	47	-	1	0
0	23	-	0	1
1	1	2	1	-2
2	0	23		

Also gilt $ggT(47, 23) = 1 = 1 \cdot 47 - 2 \cdot 23$. Wegen $1|31$ ist sie lösbar, wobei wir die Lösung mittels Multiplikation mit 31 erhalten. Dann gilt $31 \cdot 47 - 62 \cdot 23 = 31$. Daraus ergibt sich für die Kongruenz die Lösung $x \equiv -62 \equiv 32 \bmod 47$.

(b) Bestimme das multiplikative Inverse von 19 mod 71.

Auch hier erhalten wir die Lösung mittels des Euklidischen Algorithmus. Denn wir suchen die Restklasse x, so dass $19x \equiv 1 \bmod 71$ gilt. Analog zur Vorgehensweise in Teilaufgabe a) lösen wir daher die Diophantische Gleichung $71x + 19y = 1$, ebenfalls mit dem Tabellenschema:

n	r_n	q_n	x_n	y_n
-1	71	-	1	0
0	19	-	0	1
1	14	3	1	-3
2	5	1	-1	4
3	4	2	3	-11
4	1	1	-4	15
5	0	4		

So gilt $ggT(71, 19) = 1 = -4 \cdot 71 + 15 \cdot 19$, und daraus erhalten wir $(19 \bmod 71)^{-1} = 15 \bmod 71$.
(8 Punkte)

5. Es gilt $839 \in \mathbb{P}$, $840 = 2^3 \cdot 3 \cdot 5 \cdot 7$ und $841 = 29^2$.

(a) Bestimme den Wert der Eulerschen φ- Funktion dieser drei Zahlen.

Es gilt aufgrund der Rechenregeln für die Eulersche φ- Funktion

$$\begin{aligned}
\varphi(839) &= 838 \\
\varphi(840) &= \varphi(2^3 \cdot 3 \cdot 5 \cdot 7) = 840 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) \\
&= 840 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 192 \\
\varphi(839) &= \varphi(29^2) = 29^2 \cdot \left(1 - \frac{1}{29}\right) = 29^2 \cdot \frac{28}{29} = 28 \cdot 29 = 812.
\end{aligned}$$

(b) Berechne 29^{1696} mod 839.

Mit dem Satz von Euler folgt

$$29^{1696} \equiv 29^{20+2\cdot 838} \equiv 29^{20} \equiv (29^2)^{10} \equiv 2^{10} \equiv 1024 \equiv 186 \bmod 839$$

mit $29^2 = 841 \equiv 2 \bmod 839$. (7 Punkte)

6. Für einen Primteiler der zusammengesetzten Mersenne- Zahl M_{251} muss $251|(p-1)$ gelten.

(a) Bestimme die kleinste Primzahl dieser Art.

Aus $251|(p-1)$ folgt $p \equiv 1 \bmod 251$. Sowohl 1 als auch 252 sind keine Primzahlen. Der nächste Kandidat ist die 503. Mittels Probedivision durch die infragekommenden Teiler $d \leq [\sqrt{503}]$ zeigen wir, dass $503 \in \mathbb{P}$ gilt. Wegen $503 < 529 = 23^2$ genügt es, die Primzahlen bis 19 zu untersuchen.
Wegen $Q(503) = 5 + 3 = 8$ und $3 \not| 8$ ist 3 kein Teiler von 503. Wegen $503 \equiv 3 \not\equiv 0 \bmod 5$ gilt auch $5 \not| 503$. Mittels Probedivision zeigt man auch $7 \not| 503$, $11 \not| 503$, $13 \not| 503$, $17 \not| 503$ und $19 \not| 503$. Also ist 503 prim und erfüllt damit als kleinstes p die gegebene Bedingung.

(b) Zeige, dass diese Primzahl auch ein Teiler von M_{251} ist.

Damit $p|M_{251}$ gilt, muss $M_{251} = 2^{251} - 1 \equiv 0 \bmod 503$ gelten. Folglich untersuchen wir $2^{251} \bmod 503$. Es gilt $2^9 = 512 \equiv 9 \bmod 503$. Damit erhalten wir

$$\begin{aligned} 2^{18} &\equiv 9^2 \equiv 81 \equiv 3^4 \bmod 503 \\ 2^{36} &\equiv 3^8 \equiv 3^6 \cdot 3^2 \equiv 226 \cdot 9 \equiv 22 \bmod 503 \\ 2^{72} &\equiv 22^2 \equiv 484 \equiv -19 \bmod 503 \\ 2^{144} &\equiv (-19)^2 \equiv 361 \equiv -142 \bmod 503. \end{aligned}$$

Wgen $252 = 144 + 72 + 36$ gilt

$$2^{252} \equiv 2^{144+72+36} \equiv 2^{144} \cdot 2^{72} \cdot 2^{36} \equiv (-142) \cdot (19) \cdot 22 \equiv (-142) \cdot 85 \equiv 2 \bmod 503.$$

Aus $2^{252} \equiv 2 \bmod 503$ folgt $2^{251} \equiv 1 \bmod 503$ und damit die Behauptung. (8 Punkte)

7. An welchen Wochentagen fanden folgende Ereignisse statt?

(a) die Stürmung der Lufthansa- Maschine Landshut in Mogadischu (18. Oktober 1977)

Mittels der Kalenderformel $t + f(m) + g(j) \bmod 7$ gilt

$$w \equiv 18 + 6 + 1977 + \left[\frac{1977}{4}\right] - \left[\frac{1977}{100}\right] + \left[\frac{1977}{400}\right] \equiv -1 + 494 - 19 + 4 \equiv 478 \equiv 2 \bmod 7.$$

Die GSG 9 befreite die Geiseln also an einem Dienstag.

(b) der Orkan Lothar (26. Dezember 1999)

Analog erhalten wir hier

$$w \equiv 26 + 4 + 1999 + \left[\frac{1999}{4}\right] - \left[\frac{1999}{100}\right] + \left[\frac{1999}{400}\right] \equiv 2001 + 499 - 19 + 4 \equiv 0 \bmod 7.$$

Einer der schwersten Orkane Mitteleuropas verursachte Schäden in Milliardenhöhe. Der zweite Weihnachtsfeiertag war demnach ein Sonntag.

Hinweis:
Es gilt dabei für den Oktober $f(8) = 6$ und für den Dezember $f(10) = 4$. (6 Punkte)

8. Bestimme die Faktorisierung der Zahl 1729 mittels des Pollard- Rho- Verfahrens.

   Wenn wir das einfachste Beispiel mit $F(X \bmod N) = (X^2 + 1) \bmod N$ sowie $X_0 = 0$ nehmen, erhalten wir

i	X_i	Y_i	$Y_i - X_i$	$d_i = ggT(Y_i - X_i, N)$
0	0	0	0	1729
1	1	2	1	1
2	2	26	24	1
3	5	145	140	7

   Also ist 7 ein Teiler von 1729, woraus sich $1729 = 7 \cdot 247$ ergibt. Auch dies wollen wir noch mit derselben Methode faktorisieren.

i	X_i	Y_i	$Y_i - X_i$	$d_i = ggT(Y_i - X_i, N)$
0	0	0	0	247
1	1	2	1	1
2	2	26	24	1
3	5	27	22	1
4	26	122	96	1
5	183	27	156	13

   Mittels Division erhalten wir nun als Faktorisierung $1729 = 7 \cdot 13 \cdot 19$. (6 Punkte)

9. (a) Bestimme die kleinste positive Zahl, die die folgenden Eigenschaften erfüllt:

$$\begin{aligned} x &\equiv 4 \bmod 5 \\ x &\equiv 2 \bmod 11 \\ x &\equiv 1 \bmod 12^2. \end{aligned}$$

   Wir definieren nun $n_1 = 5$, $n_2 = 11$ und $n_3 = 12^2$, welche paarweise teilerfremd sind bzw. $n = 5 \cdot 11 \cdot 12^2 = 7920$. Außerdem ist $a_1 = 4$, $a_2 = 2$ und $a_3 = 1$. Dann berechnen wir

$$\begin{aligned} N_1 &:= \frac{n}{n_1} = 11 \cdot 12^2 = 1584 \\ N_2 &:= \frac{n}{n_2} = 5 \cdot 12^2 = 720 \\ N_3 &:= \frac{n}{n_3} = 5 \cdot 11 = 55. \end{aligned}$$

   Das Inverse von N_k mit $k = 1, 2, 3$ berechnet man über

$$\begin{aligned} 1584 \cdot N_1^{-1} &\equiv 1 \bmod 5 \Leftrightarrow -1 \cdot N_1^{-1} \equiv 1 \bmod 5 \Leftrightarrow N_1^{-1} \equiv -1 \bmod 5 \\ 720 \cdot N_2^{-1} &\equiv 1 \bmod 11 \Leftrightarrow 5 \cdot N_2^{-1} \equiv 1 \bmod 11 \Leftrightarrow N_2^{-1} \equiv 9 \equiv -2 \bmod 11 \\ 55 \cdot N_3^{-1} &\equiv 1 \bmod 12^2 \Leftrightarrow N_3^{-1} \equiv 55 \bmod 12^2. \end{aligned}$$

   Damit folgt für eine Lösung x_0

$$x_0 = \sum_{k=1}^{3} N_k \cdot N_k^{-1} a_k = 4 \cdot 1584 \cdot (-1) + 2 \cdot (-2) \cdot 720 + 55 \cdot 1 \cdot 55 = -6191.$$

   Die allgemeine Lösung ergibt sich aus $x_m = -6191 + 7920m$ mit $m \in \mathbb{Z}$.
   Mit $m = 1$ ergibt sich als Ergebnis $x_1 = 1729$.

(b) Stellt die Lösung eine Carmichael- Zahl dar (mit Begründung)?

Aus Aufgabe 8 kennen wir bereits die Faktorisierung von $1729 = 7 \cdot 13 \cdot 19$. Somit ist die ungerade Zahl 1729 zumindst ein Produkt aus mindestens drei Primfaktoren und quadratfrei. Wir haben noch $(p-1)|((n-1)$ für jeden Primfaktor nachzuweisen.
Es gilt $7 - 1 = 6|1728$, da 1728 gerade ist und $Q(1728) = 18$ durch 3 teilbar ist.
Wegen $1728 \equiv 0 \bmod 4$ gilt auch $13 - 1 = 12|1728$.
Schließlich ist auch $19 - 1 = 18|1728$, da auch $3|\frac{1728}{3} = 576$ wegen $Q(576) = 18$ erfüllt ist.
Damit ist 1729 eine Carmichael- Zahl. (9 Punkte)

10. Zeige, dass die Diophantische Gleichung $x^6 - 11x^4 + 36x^2 - 36 + 27^n = 0$ für alle $n \in \mathbb{N}$ unlösbar ist.

Wir betrachten die Gleichung modulo 27. Dann gilt

$$x^6 - 11x^4 - 9x^2 - 9 \equiv 0 \bmod 27.$$

Teilbarkeit durch $27 = 3^3$ impliziert auch Teilbarkeit durch 3, also gilt auch

$$x^6 - 11x^4 - 9x^2 - 9 \equiv x^6 - 2x^4 \equiv x^6 + x^4 \equiv 0 \bmod 3.$$

Mit dem Satz von Euler gilt mit $x^3 \equiv x \bmod 3$ somit $x^2 + x^2 \equiv 2x^2 \bmod 3$. Dies wird nur von der Restklasse 0 mod 3 gelöst. Also gilt $x = 3k$ mit einem $k \in \mathbb{Z}$. Daraus folgt

$$(3k)^6 - 11 \cdot (3k)^4 + 9 \cdot (3k)^2 - 9 \equiv 3^6 \cdot k^6 - 3^4 \cdot 11k^4 + 3^4 \cdot k^2 - 9 \equiv -p \not\equiv 0 \bmod 27.$$

Damit ist die Kongruenz modulo 27 und damit auch die gegebene Diophantische Gleichung unlösbar. (8 Punkte)

11. (a) Berechne $\mathrm{ord}_{13} 3$ und zeige, dass 3 keine Primitivwurzel modulo 13 ist.

Es gilt $\mathrm{ord}_{13} 3|\varphi(13) = 12$, weswegen es genügt, die Menge $\{1, 2, 3, 4, 6, 12\}$ zu untersuchen. Es ist $3^2 \equiv 9 \bmod 13$ und $3^3 \equiv 1 \bmod 13$. Somit gilt $\mathrm{ord}_{13} 3 = 3$, und wegen $3 < 12 = \varphi(13)$ ist 3 keine Primitivwurzel modulo 13.

(b) Bestimme eine Primitivwurzel modulo 13.

Es gilt etwa

$$\begin{aligned} 2^1 &\equiv 2 \not\equiv 1 \bmod 13 \\ 2^2 &\equiv 4 \not\equiv 1 \bmod 13 \\ 2^3 &\equiv 8 \not\equiv 1 \bmod 13 \\ 2^4 &\equiv 3 \not\equiv 1 \bmod 13 \\ 2^6 &\equiv -1 \not\equiv 1 \bmod 13. \end{aligned}$$

Nach dem kleinen Fermat gilt $2^{12} \equiv 1 \bmod 13$, womit 2 eine Primitivwurzel modulo 13 ist.

(c) Stelle jedes $g \in (\mathbb{Z}/13\mathbb{Z})^*$ als Potenz der in Teilaufgabe b) gefundenen Primitivwurzel dar.

Nun gilt mit den Erkenntnissen aus Teilaufgabe b)

g	1	2	3	4	5	6	7	8	9	10	11	12
2^k	2^{12}	2^1	2^41	2^2	2^9	2^5	2^{11}	2^3	2^8	2^{10}	2^7	2^6

(d) Löse die Kongruenz $x^5 \equiv 11 \bmod 13$.

Die Kongruenz $x^5 \equiv 11 \bmod 13$ ist zur linearen Kongruenz $5j \equiv 7 \bmod 12$ äquivalent. Lösen dieser Kongreunzz ergibt $j \equiv 11 \bmod 12$ und damit $x \equiv 7 \bmod 13$

(e) Löse die Kongruenz aus Teilaufgabe d) mit der Methode der schnellen Exponentiation.

Es gilt $ggT(11, 13) = 1$ und auch $ggT(5, \varphi(13)) = 1$. damit bestimmen wir $5u - 12v = 1$, woraus wir $u = 5$ erhalten. Damit ist $x \equiv 11^5 \equiv (-2)^5 \equiv -32 \equiv 7 \bmod 13$. (12 Punkte)

12. Es seien $n \in \mathbb{N}$ ungerade mit $n \geq 2$ und $m \in \mathbb{N}_0$.

(a) Zeige, dass $(n - 1 + n \cdot m)^{n-1} \equiv 1 \bmod n$ gilt.

Es gilt

$$\begin{aligned}(n-1+nm)^{n-1} &= \sum_{k=0}^{n-1} \binom{n-1}{k} (n-1)^k (nm)^{n-1-k} \\ &= \underbrace{\sum_{k=0}^{n-2} \binom{n-1}{k} (n-1)^k (nm)^{n-1-k}}_{\equiv 0 \bmod n} + \binom{n-1}{n-1} (n-1)^{n-1} \\ &\equiv (-1)^{n-1} \equiv 1 \bmod n,\end{aligned}$$

da $n - 1$ gerade ist.

(b) Folgt daraus, dass n eine Pseudoprimzahl zur Basis $n - 1 + n \cdot m$ ist?

Nein, diese Aussage gilt für alle ungeraden Zahlen und ist damit als Beweismittel für eine Pseudoprimzahl untauglich. (6 Punkte)

13. Es sei $n = pq$ mit $p = 17$ und $q = 19$.
Als öffentlichen Schlüssel wähle ein Teilnehmer eines RSA- Systems $(e, n) = (11, 323)$ und versende die Botschaft $C = 3$. Bestimme den Klartext B.

Es gilt $\varphi(n) = (p-1)\cdot(q-1) = 16 \cdot 18 = 288$. Für den größten gemeinsamen Teiler von e und $\varphi(n)$ gilt somit auch $ggT(11, 288) = 1$, und wir müssen nun ein $d > 0$ bestimmen, so dass $ed \equiv 1 \bmod \varphi(n)$ ist. Dies erhalten wir mit Hilfe des Euklidischen Algorithmus anhand der Gleichung $288x + 11y = 1$ und dem Tabellenschema

n	r_n	q_n	x_n	y_n
-1	288	-	1	0
0	11	-	0	1
1	2	26	1	-26
2	1	5	-5	131
3	0	2		

Also ist $ggT(288, 11) = 1 = -5 \cdot 288 + 131 \cdot 11$. Das gesuchte d ist also $d = 131$.
Die gesuchte ursprüngliche Botschaft B können wir mittels $C^d \equiv B \bmod n$, also $3^{131} \bmod 323$ berechnen. Es gilt

$$\begin{aligned}3^1 &\equiv 3 \bmod 323,\ 3^2 \equiv 9 \bmod 323,\ 3^4 \equiv 81 \bmod 323, 3^8 \equiv 101 \bmod 323 \\ 3^{16} &\equiv -135 \bmod 323,\ 3^{32} \equiv 137 \bmod 323,\ 3^{64} \equiv 35 \bmod 323, 3^{128} \equiv 256 \bmod 323.\end{aligned}$$

Daher folgt mit $ggT(C, n) = ggT(3, 323) = 1$ nun auch $3^{131} = 3 \cdot 9 \cdot 256 \equiv 3^3 \cdot 2^8 \equiv 129 \bmod 323$.
Also ist die gesuchte Botschaft $B = 129$. (6 Punkte)

14. Michael und Vito wollen einen geheimen Schlüssel vereinbaren. Sie wählen dazu $p = 23$ und $r = 5$. Michael wählt $a \in \{1, 2, \ldots, 22\}$, Vito $b \in \{1, 2, \ldots, 22\}$. Damit berechnen sie $A = r^a \equiv 2 \bmod 23$ und $B = r^b \equiv 3 \bmod 23$.

(a) Bestimme a und b mit dem diskreten Logarithmus.

Es lässt sich nun jedes Element aus $(\mathbb{Z}/23\mathbb{Z})^*$ als eine Potenz von $r = 5$ darstellen. Zusammengefasst in einer Tabelle ergibt sich

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
5^k	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	...

Damit lässt sich nun die diskrete Logarithmusfunktion

$$\mathrm{dlog}_r \colon (\mathbb{Z}/23\mathbb{Z})^* \to (\mathbb{Z}/23\mathbb{Z})^*, \quad r^i \to i \bmod 22$$

definieren. Wir erhalten $a = \mathrm{dlog}_r(A) = \mathrm{dlog}_5(2) = 2$ und $b = \mathrm{dlog}_r(B) = \mathrm{dlog}_5(3) = 16$.

(b) Berechne den geheimen Schlüssel k.

Um den geheimen Schlüssel k bestimmen zu können, ist wegen $k \equiv A^b \equiv B^a \bmod p$ entweder $2^{16} \bmod 23$ oder $3^2 \bmod 23$ zu berechnen. Es ergibt sich $k = 9$.

Mit Vitos öffentlichem Schlüssel $(23, 5, 3)$ möchte Michael ihm nun geheime Nachrichten verschicken. Mit dem geheimen Schlüssel k bestimmt er zuerst das Paar $(c_1, c_2) = (5^k \bmod 23, mB^k \bmod 23)$. Marta möchte die Nachricht ebenfalls lesen, kann aber nur $c_2 = 19$ abfangen und ohne Kenntnis des geheimen Schlüssels k die Nachricht nicht entschlüsseln.

(c) Bestimme den Klartext m.

Der erste Teil der Nachricht lässt sich mit Kenntnis des geheimen Schlüssels k errechnen. Es ist $c_1 \equiv r^k \equiv 5^9 \equiv 11 \bmod 23$. Zum Entschlüsseln der Nachricht bestimmen wir nun $(c_1^b)^{-1} \equiv (11^{16})^{-1} \bmod 23$ und multiplizieren dies mit der Botschaft. Nun gilt

$$\begin{aligned} 11^2 &\equiv 121 \equiv 6 \bmod 23 \\ 11^4 &\equiv 36 \equiv 13 \bmod 23 \\ 11^8 &\equiv 169 \equiv 8 \bmod 23 \\ 11^{16} &\equiv 64 \equiv 18 \equiv -5 \bmod 23. \end{aligned}$$

Die Inverse von $-5 \bmod 31$ ist wegen $5 \cdot 14 = 70 = 3 \cdot 23 + 1$ gerade $-14 \equiv 9 \bmod 23$. Es genügt daher, $9c_2 \bmod 23$ zu bestimmen, woraus wir $9 \cdot 19 \equiv 171 \equiv 10 \bmod 23$ erhalten. (12 Punkte)

15. Überprüfe, ob $1241 = 17 \cdot 73$ ein quadratischer Rest modulo der Primzahl 4801 ist.

Es gilt wegen $4801 \equiv 73 \equiv 17 \equiv 1 \bmod 4$ und $7 \equiv 3 \bmod 4$

$$\begin{aligned} \left(\frac{1241}{4801}\right) &= \left(\frac{17}{4801}\right) \cdot \left(\frac{73}{4801}\right) = \left(\frac{4801}{17}\right) \cdot \left(\frac{4801}{73}\right) = \left(\frac{7}{17}\right) \cdot \left(\frac{56}{73}\right) \\ &= \left(\frac{17}{7}\right) \cdot \left(\frac{7}{73}\right) \cdot \left(\frac{2^3}{73}\right) = \left(\frac{3}{7}\right) \cdot \left(\frac{73}{7}\right) \cdot \left(\frac{2^2}{73}\right) \cdot \left(\frac{2}{73}\right) \\ &= \left(\frac{3}{7}\right) \cdot \left(\frac{3}{7}\right) \cdot (-1)^{\frac{73^2-1}{8}} = (-1)^{\frac{73^2-1}{8}} = 1. \end{aligned}$$

Damit ist 1241 ein quadratischer Rest modulo 4801. (4 Punkte)

Viel Erfolg!