Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Theresa Kumpitsch

Elementare Zahlentheorie

Wintersemester 2021/22

Übungsblatt 8 10.12.21

Bemerkung: Bei Teilaufgaben, die mit * gekennzeichnet sind, handelt es sich um Programmieraufgaben, welche von der regulären Bewertung ausgeschlossen sind. Hierfür kann man je zwei Bonuspunkte für die Angabe des Codes, sowie einen Bonuspunkt für das richtige Ergebnis erhalten.

Aufgabe 1 (Unendlich viele Primzahlen (in arithmetischer Progression), 5 Punkte)**.**
Sei G eine echte Untergruppe der multiplikativen Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$.

(a) Zeigen Sie, dass wenn N eine ganze Zahl mit $(N, m) = 1$ ist, dessen Restklasse mod m kein Element von G ist, dann besitzt N einen Primfaktor, dessen Restklasse kein Element von G ist.

(b) Gegeben eine endliche Menge an Primzahlen $p_1, \dots, p_r$, die nicht m teilen, und eine Restklasse $b \bmod m$. Zeigen Sie, dass es eine ganze Zahl N gibt, sodass $N \equiv b \bmod m$ und die teilerfremd zu allen $p_1, \dots, p_r$ ist.

(c) Zeigen Sie, dass es unendlich viele Primzahlen gibt, dessen Restklassen mod m nicht in G liegen.
Tipp: Angenommen, es gibt nur endlich viele solche Primzahlen $p_1, \dots, p_r$. Wählen Sie eine passende Restklasse b und N wie in (b) und folgern Sie die Behauptung mit Hilfe von (a).

(d) Folgern Sie, dass es unendlich viele Primzahlen in mindestens zwei arithmetischen Progressionen $3 \bmod 8, 5 \bmod 8$ und $7 \bmod 8$ gibt.

Aufgabe 2 (Primitivwurzeln, 5 (+3) Punkte)**.**

(a) Bestimmen Sie alle Primitivwurzeln modulo 11, 13 und 17.

(b) Zeigen Sie: Es gibt keine Primzahl p, so dass 4 eine Primitivwurzel modulo p ist.

(c) Sei $p > 0$ eine Primzahl, $k > 0$ und sei w eine Primitivwurzel modulo p^k. Zeigen Sie:
  (i) Ist w ungerade, so ist w eine Primitivwurzel modulo $2p^k$,
  (ii) Ist w gerade, so ist $w + p^k$ eine Primitivwurzel modulo $2p^k$.
  (iii) Bestimmen Sie eine Primitivwurzel modulo $n = 98$.

(d)* Nutzen Sie ein Computeralgebrasystem (z.B. SageMath[1]), um die kleinste Primzahl zu berechnen, für die die kleinste Primitivwurzel größer als 100 ist.

Bemerkung: Man kann zeigen, dass es genau dann Primitivwurzeln mod n gibt, wenn $n = 1, 2, 4, p^k$ oder $2p^k$, wobei p eine ungerade Primzahl sei.

Aufgabe 3 (Der diskrete Logarithmus, 3 Punkte)**.** Es sei m ein Modulus, so dass $(\mathbb{Z}/m\mathbb{Z})^\times$ eine Primitivwurzel w besitzt. Der diskrete Logarithmus von $(\mathbb{Z}/m\mathbb{Z})^\times$ ist durch die Abbildung

$$\log_w \colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}/\varphi(m)\mathbb{Z}$$
$$w^j \bmod m \mapsto j \bmod \varphi(m)$$

definiert. Zeigen Sie, dass $\log_w$ ein Gruppenisomorphismus ist, d.h.:

(a) $\log_w$ ist wohldefiniert,

(b) $\log_w$ erfüllt $\log_w(a \cdot b) = \log_w(a) + \log_w(b)$,

(c) $\log_w$ ist bijektiv.

[1]Das ist für diese Aufgabe besonders geeignet. Siehe https://doc.sagemath.org/html/en/prep/Quickstarts/Number-Theory.html für eine kurze Übersicht relevanter Befehle. Es ist nicht notwendig, SageMath zu installieren. Für den Zweck dieses Übungsblatt reicht auch https://sagecell.sagemath.org/.

Aufgabe 4 (RSA-Verfahren – Nachrichten entschlüsseln, 5 Punkte)**.**
Bob ist auf einer Weihnachtsfeier ganz begeistert von den Keksen, die Alice mitgebracht hat. Da es sich um ein altes Familienrezept handelt, will Alice die geheime Zutat eigentlich nicht verraten. Da Bob jedoch nicht eher Ruhen kann, bis er das Geheimnis dieser köstlichen Kekse kennt, stimmt Alice zu, ihm die Zutat verschlüsselt zu senden. Deshalb hat Bob einen öffentlichen RSA-Schlüssel $(n, e) = (4141, 127)$ ausgegeben und Alice hat ihre RSA-verschlüsselte Nachricht an Bob gesendet. Inzwischen haben Sie doch einen Zugriff auf diese Nachricht, die folgendermaßen lautet:

3460 1222 202 1582 499

Können Sie diese hacken? Was ist die geheime Zutat?

Erläuterung: Zur Verschlüsselung werden die Buchstaben gemäß folgender Tabelle in Zahlen umgewandelt. Anschließend wurde die Ziffernfolge in 4-stellige Blöcke unterteilt. Bei Bedarf wird der letzte Block mit Leerzeichen " " = 36 aufgefüllt.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Tipp: Sie sollten für diese Aufgabe einen Computer benutzen.

Aufgabe 5 (RSA-Verfahren – Einfache Attacken, 2 (+3) Punkte)**.**
Aus der Vorlesung ist bekannt: Ist die Faktorisierung des RSA-Modulus n bekannt, so lässt such das zugehörige RSA-Kryptosystem knacken. In gewissen Situationen ist das einfach, z.B. wenn $\varphi(n)$ bekannt ist. Wir betrachten hier den Fall, dass p und q"nah" sind. Schreibe $n = pq$ mit p, q Primzahlen.

(a) Setzen Sie

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2, \quad t = \frac{p+q}{2}, s = \frac{p-q}{2}.$$

Angenommen, p und q liegen nah beieinander. Überlegen Sie sich eine Strategie t (algorithmisch) zu bestimmen. Erklären Sie, wie Sie dadurch die Faktoren p und q bestimmen können.

(ii)* Implementieren Sie (z.B. in SageMath) einen Algorithmus, der einen RSA-Modulus n faktorisiert, wenn einer der Faktoren etwa die Größe $\sqrt{n}$ hat Faktorisieren Sie damit $n = 23360947609$.

Abgabe: Am kommenden Freitag, den **17.12.21**, bis um 12:00 digital auf OLAT.