Wolfgang K. Seiler
Tel. 2515

A5, C201

8. Mai 2014

Probeklausur zur Zahlentheorie

• • • **Schreiben Sie bitte auf jedes Blatt Ihren Namen!** • • •

Aufgabe 1: *(4 Punkte)*

a) Heute vor 65 Jahren, am 8. Mai 1949, verabschiedete der Parlamentarische Rat das Grundgesetz für die Bundesrepublik Deutschland. An welchem Wochentag geschah dies?

b) Heute in 65 Jahren ist der 8. Mai 2079. Auf welchen Wochentag fällt dieser?

Aufgabe 2: *(12 Punkte)*

a) Bestimmen Sie den größten gemeinsamen Teiler von 1111 und 2552, und stellen Sie diesen als ganzzahlige Linearkombination dieser beiden Zahlen dar!

b) Zeigen Sei: Eine zweistellige Zahl ist genau dann prim, wenn sie nicht durch zwei, drei, fünf oder sieben teilbar ist.

c) Geben Sie die Primfaktorzerlegung von 1111 und 2552 an! Dabei muß nur für Faktoren größer fünfzig bewiesen werden, daß es sich tatsächlich um Primzahlen handelt.

d) Bestimmen Sie alle $(x, y) \in \mathbb{Z}^2$ mit $1111x + 2552y = 111$!

e) Bestimmen Sie alle $(x, y) \in \mathbb{Z}^2$ mit $1111x + 2552y = 121$!

Aufgabe 3: *(7 Punkte)*

a) Finden Sie in $\left(\mathbb{Z}/1009\mathbb{Z}\right)^\times$ ein Element x, für das $15x = 22$ ist!

b) Was ist $2^{20} \bmod 1009$?

c) Zeigen Sie, daß die Zwei eine primitive Wurzel modulo 29 ist!

Aufgabe 4: *(6 Punkte)*

a) $N = pqr$ sei ein Produkt dreier paarweise verschiedener Primzahlen. Zeigen Sie, daß für *jede* natürliche Zahl a gilt: $a^{(p-1)(q-1)(r-1)+1} \equiv a \bmod N$!

b) Gilt dies auch, wenn man $(p-1)(q-1)(r-1)$ durch irgendein gemeinsames Vielfaches von $p-1$, $q-1$ und $r-1$ ersetzt?

• • • **Bitte wenden!** • • •

Aufgabe 5: *(7 Punkte)*

a) Die Zahl $N = 25\,591$ ist Produkt zweier ungefähr gleich großer Primzahlen. Finden Sie diese!

b) Finden Sie den kleinstmöglichen RSA-Exponenten e zum RSA-Modul N!

c) Finden Sie zu diesem Exponenten e einen privaten Exponenten d!

Aufgabe 6: *(4 Punkte)*

a) Zeigen Sie: Die Anzahl der Nullen, mit denen die Zahl $n!$ endet, ist $\sum_{i=1}^{\infty} \left[\frac{n}{5^i}\right]$!

b) Wie viele Nullen stehen am Ende von $1000!$?

Aufgabe 7: *(4 Punkte)*

a) Was ist eine CARMICHAEL-Zahl?

b) Zeigen Sie, daß 1105 eine CARMICHAEL-Zahl ist! (*Hinweis:* $13 \cdot 17 = 221$)

Aufgabe 8: *(8 Punkte)*

a) Faktorisieren Sie $N = 7991$ mit POLLARDS $(p-1)$-Methode mit Suchgrenze $B = 6$ und der Basis $a = 2$!

b) Welche Bedingung muß die Suchgrenze B erfüllen, damit POLLARDS Methode für 7991 zum Erfolg führt?

Aufgabe 9: *(8 Punkte)*

a) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{12}$!

b) Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 12y^2 = 1$!

c) Was ist $x = [2; \overline{2}] = [2; 2, 2, 2, \dots] = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}}$?

Abgabe bis zum Donnerstag, dem 8. Mai 2014, um 13^{30} Uhr

• • • **Steht Ihr Name auf jedem Blatt?** • • •