Mathematisches Institut
Abt. für Reine Mathematik
Dr. K. Halupczok

22.06.2006

Übungen zur Vorlesung

Elementare Zahlentheorie

SoSe 2006

Musterlösung Blatt 7

Aufgabe 1.

(a) *Bestimme alle Lösungen der Kongruenz* $x^3 - 2x + 4 \equiv 0\ (125)$.

Beh.: Alle Lösungen der Kongruenz $x^3-2x+4 \equiv 0\ (125)$ sind $8, 33, 58, 83, 108$, $23, 48, 73, 98, 123$ und 69.

Bew.: Sei $f(x) := x^3 - 2x + 4$, dann ist $f'(x) = 4x^2 - 2$. Alle Lösungen von $f(x) \equiv 0\ (5)$ sind 3 und 4.

(a) Lösungen 3 mod 5: $f'(3) \equiv 0\ (5)$ und $f(3) \equiv 0\ (25) \rightsquigarrow 3 + b \cdot 5$ mit $b = 0, 1, 2, 3, 4$ sind alle Lösungen mod 25 (2.Fall Satz).
also: **3,8,13,18,23**.

(b) Lösungen 4 mod 5: $f'(4) = 46 \equiv 1\ (5) \rightsquigarrow$ nur eine Lösung mod 25:
Ansatz: $\frac{f(4)}{5} + b \cdot f'(4) \equiv 0\ (5) \rightsquigarrow 12 + b \equiv 0\ (5) \rightsquigarrow b \equiv 3\ (5)$.
Somit $4 + b \cdot 5 =$ **19** Lösung mod 25.

(c) Aufstieg von den Lösungen mod 25 zu denen mod 125:

Lsg. 3 mod 25: $f'(3) \equiv 0\ (5)$ und $f(3) = 25 \not\equiv 0\ (125) \rightsquigarrow$ Keine Lösung mod 125

Lsg. 8 mod 25: $f'(8) = 190 \equiv 0\ (5)$ und $f(8) = 500 \equiv 0\ (125) \rightsquigarrow$ Lösungen $8 + b \cdot 25$ mit $b = 0, \ldots, 4$, also **8,33,58,83,108** mod 125.

Lsg. 13 mod 25: $f'(13) = 505 \equiv 0\ (5)$ und $f(13) = 2175 \not\equiv 0\ (125) \rightsquigarrow$ keine Lösung mod 125

Lsg. 18 mod 25: $f'(18) = 1585 \equiv 0\ (5)$ und $f(18) = 5800 \not\equiv 0\ (125) \rightsquigarrow$ keine Lösung mod 125

Lsg. 23 mod 25: $f'(23) = 1585 \equiv 0\ (5)$ und $f(23) = 12125 \equiv 0\ (125) \rightsquigarrow$ Lösungen $23 + b \cdot 25$ mit $b = 0, \ldots 4$, also **23,48,73,98,123** mod 125

Lsg. 19 mod 25: $f'(19) = 1081 \not\equiv 0(5) \rightsquigarrow$ nur eine Lösung mod 125:
Ansatz: $\frac{f(19)}{25} + b \cdot f'(19) \equiv 0\ (5) \rightsquigarrow 273 \cdot b \cdot 1081 \equiv 0\ (5) \rightsquigarrow 3 + b \equiv 0\ (5) \rightsquigarrow b = 2$
Liefert die Lösung $19 + b \cdot 25 =$ **69** mod 125

(b) *Sei p prim. Bestimme alle Lösungen der Kongruenz* $x^{p-2} + \cdots + x + 1 \equiv 0\ (p)$.

Beh.: p prim $\Rightarrow$ die Kongruenz $x^{p-2} + \cdots + x + 1 \equiv 0\ (p)$. hat die Lösungen $2, \ldots, p-1$

Bew.: Sei $f(x) := x^{p-2}+\cdots+x+1 \rightsquigarrow (x-1)f(x) = x^{p-1}-1$ laut geometrischer Summen-Formel. Da p prim, hat $x^{p-1}-1 \equiv 0\ (p)$ nach Fermat die $p-1$ Lösungen $1, \ldots, p-1$. Ist $x \not\equiv 1\ (p)$ und $x^{p-1}-1 \equiv 0\ (p)$, so folgt $f(x) \equiv 0\ (p)$, also hat $f(x) \equiv 0\ (p)$ mindestens $p-2$ Lösungen. Da $\deg f = p-2$, hat die Kongruenz nach Lagrange genau $p-2$ Lösungen, nämlich $2, \ldots, p-1$.

Aufgabe 2. *Bestimme ohne Rechnereinsatz den Rest von* $\dfrac{70!}{18}$ *nach Division durch* 71.

Beh.: $\frac{70!}{18} \equiv 67\ (71)$

Bew.: Nach Wilson gilt $70! \equiv -1\ (71)$, da 71 prim. Es läßt sich auf der rechten Seite ein Vielfaches von 71 zufügen, also betrachten wir ein $71k-1$, das durch 18 teilbar ist. Damit wird $\frac{71k-1}{18}\ (71)$ der gesuchte Rest sein. Bestimmung von k als Lösung von $71k \equiv 1\ (18)$:
Inverses von $71 \equiv -1\ (18)$ ist -1, also ist $k = -1$ Lösung und $\frac{-71-1}{18} = -4 \equiv 67\ (71)$ der gesuchte Rest.

Aufgabe 3.

Zeige den Satz von Wilson für Primzahlzwillinge:
Sei $n \geq 2$, dann sind äquivalent:

(a) n und $n+2$ sind Primzahlen,
(b) $4((n-1)!+1)+n \equiv 0 \pmod{n(n+2)}$.

Hinweis: $n(n+1) \equiv (-2)(-1) \pmod{n+2}$.

Beh.: Aussagen a) und b) sind für $n \geq 2$ äquivalent.

Bew.: „$\Leftarrow$“ Gelte b). Annahme: n oder $n+2$ nicht prim.

Fall (α) $n = p \cdot k, p$ prim, $p < n$: Dann folgt $p \mid n$, $p \mid (n-1)!$, und aus b) also $p \mid 4$; also ist n eine 2-er Potenz. Mit $n = 2^l$ folgt $2^{l+1} \mid 4((2^l-1)!+1) + 2^l = 2^2 \cdot (2^{l-2} + (2^l-1)! + 1)$, wobei $(2^{l-2} + (2^l-1)! + 1)$ ungerade für $l \geq 3$ im Widerspruch zur Aussage, also ist $n = 2$ oder $n = 4$, aber dafür gilt b) nicht. Also ist n prim.

Fall (β) $n+2 = q \cdot l, q$ prim, $q < n+2$: Dann folgt $q \mid n+2, q \mid (n-1)!$, und aus b) also $p \mid 4$; also ist $n+2$ eine 2er-Potenz. Mit $m = 2^l-2$ folgt $2^{l+1} \mid 4((2^l-3)!+1)+2^l-2 = 2 \cdot (2 \cdot (2^l-3)!+2+2^{l-1}-1)$ wobei $(2 \cdot (2^l-3)! + 2 + 2^{l-1} - 1)$ ungerade für $l \geq 2$, ein Widerspruch. Also ist $n+2$ prim.

„⇒“ $n, n+2$ prim $\rightsquigarrow$ (Wilson)

$$\begin{aligned}(n-1)!+1 \equiv 0\ (n) &\rightsquigarrow 4((n-1)!+1)+n \equiv 0\ (n)\\ (n+1)!+1 \equiv 0\ (n+2) &\rightsquigarrow 4((n-1)!+1)+n\\ &\equiv 2(n+1)n(n-1)!+2+n+2\\ &\equiv 2((n+1)!+1)+(n+2)\\ &\equiv 0\ (n+2)\end{aligned}$$

(da $n+1 \equiv -1\ (n+2), n \equiv -2\ (n+2)$, vgl. Hinweis.)
Also: $4((n-1)!+1)+n \equiv 0\ (n(n+2))$, da $(n, n+2) = 1$ für $n > 2$ prim.

Aufgabe 4.

Zeige das folgende Primzahlkriterium: Sei $N \geq 3$ eine ungerade Zahl und sei $N-1 = \prod_{i=1}^{r} p_i^{k_i}$ die Primfaktorzerlegung von $N-1$ (p_i paarweise verschiedene Primzahlen). Genau dann ist N eine Primzahl, wenn es eine Zahl a gibt mit

$$a^{N-1} \equiv 1 \pmod{N}$$

und

$$a^{(N-1)/p_i} \not\equiv 1 \pmod{N} \quad \textit{für alle } i = 1, \ldots, r.$$

In diesem Fall ist a eine Primitivwurzel mod N.

Vor.: $N \geq 3$ ungerade, $N-1 = \prod_{i=1}^{r} p_i^{k_i}$ die PFZ von $N-1$

Beh.: N prim $\Leftrightarrow \exists a \in \mathbb{Z}$:

$$(1) \quad a^{N-1} \equiv 1 \pmod{N}$$

und

$$(2) \quad a^{(N-1)/p_i} \not\equiv 1 \pmod{N} \quad \text{für alle } i = 1, \ldots, r.$$

In diesem Fall ist a eine Primitivwurzel mod N.

Bew.: ⇒: Sei N prim, sei a eine P.W. mod N. (1) und (2) sind damit erfüllt.
⇐: Gelten (1) und (2), so folgt: $p_i^{k_i} \mid \mathrm{ord}_N(a)$ für alle $i = 1, \ldots, r$, denn:
(1) $\Rightarrow \mathrm{ord}_N \mid (N-1) \Rightarrow$ ex. s mit $s \cdot \mathrm{ord}_N(a) = N-1 = p_i \cdot \frac{N-1}{p_i} = p_i^{k_i} \cdot \prod_{j \neq i} p_j^{k_j}$, also $p_i^{k_i} \mid s \cdot \mathrm{ord}_N(a)$.
Da nun $a^{\frac{N-1}{p_i}} \not\equiv 1\ (N)$ ist ist $\mathrm{ord}_N(a) \nmid \frac{N-1}{p_i}$. Dann: $p_i \nmid s$.
(Sonst: $p_i \mid s \rightsquigarrow \frac{s}{p_i} \cdot \mathrm{ord}_N(a) = \frac{N-1}{p_i} \rightsquigarrow \mathrm{ord}_N(a) \mid \frac{N-1}{p_i}$)
Es folgt: $p_i^{k_i} \mid \mathrm{ord}_N(a)$.
Somit: $(N-1) \mid \mathrm{ord}_N(a)$, aber $\mathrm{ord}_N(a) \mid (N-1)$ nach (1), also: $\mathrm{ord}_N(a) = N-1$, d.h. $(\mathbb{Z}/N)^*$ hat mindestens $N-1$ viele Elemente. Dann ist N prim. (Denn sonst hat $(\mathbb{Z}/N)^*$ ja $\varphi(N) < N-1$ viele Elemente: $N = n \cdot m$ mit $(n, m) = 1, n, m \geq 2 \Rightarrow \varphi(N) \leq (n-1) \cdot (m-1) = N-n-m+1 < N-1$)
Somit $\mathrm{ord}_N(a) = N-1$, d.h. a ist dann auch P.W. mod N.