6. ÜBUNGSSTUNDE - 30.4.2015

(1) Zeigen Sie, dass in jedem Hauptidealbereich R es zu allen $x, y \in R$ Elemente $a, b, d \in R$ gibt mit $d|x$, $d|y$, $d = ax + by$ sowie $\forall c \in R : \ (c|x \wedge c|y) \Longrightarrow c|d$.
[Dieses d könnte man einen "maximalen gemeinsamen Teiler von x und y" nennen.]

(2) Für welche $n \in \mathbb{N}$ ist $\mathbb{Z}_n$ faktoriell? Euklidisch? Ein Hauptidealbereich? Ein Integritätsbereich?

(3) Weisen Sie nach, dass für $n = p_1^{t_1} \cdots p_k^{t_k} \in \mathbb{N}$ gilt: $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$.

(4) Wie viele 4-stellige Zahlen sind zu 10000 relativ prim?

(5) Sie fangen in einer RSA-Nachricht vom Teilnehmer mit der "Adresse" $(n, k) = (32954765761773295963, 1031)$ die 7-buchstabige Nachricht $0, 13162954373369437233, 15603885136025301867, 25727844017305265599, 1, 11812381124012446946, 0$ ab. Finden Sie diese Nachricht im Klartext. Dabei seien die Buchstaben durch $A = 0$, $B = 1, \ldots,$ $Z = 25$ codiert. [Verwenden Sie beim Decodieren in Mathematica einmal die Funktion Mod[c^d,n] und einmal PowerMod[c,d,n]; was ist der Unterschied?]. Welche Schwächen hat dieses Setup?