

**Proseminar Diskrete Mathematik  
im Sommersemester 2011  
7.Blatt für 6.5.2011**

33) Was versteht man unter dem *schnellen Potenzieren*?  
Sei  $A$  eine quadratische Matrix von Zahlen. Wieviele Matrizenmultiplikationen braucht man, um die Matrixpotenz  $A^{31}$  auszurechnen?

34) Was ist der *größte gemeinsame Teiler* bzw. das *kleinste gemeinsame Vielfache* zweier ganzer Zahlen ungleich null?  
Berechnen Sie mit dem erweiterten euklidischen Algorithmus den größten gemeinsamen Teiler von 360 und 1026 sowie ganze Zahlen  $u$  und  $v$  mit

$$360 \cdot u + 1026 \cdot v = \text{ggT}(360, 1026).$$

Was ist das kleinste gemeinsame Vielfache von 360 und 1026?

35) Wie können *Multiplikationen mit 2* und *Divisionen durch 2* effizient implementiert werden?  
Berechnen Sie mit dem binären erweiterten euklidischen Algorithmus den größten gemeinsamen Teiler von 360 und 1026 sowie ganze Zahlen  $u$  und  $v$  mit

$$360 \cdot u + 1026 \cdot v = \text{ggT}(360, 1026).$$

36) Wann ist eine Restklasse *invertierbar* ?  
Berechnen Sie für alle invertierbaren Restklassen modulo 36 die inverse Restklasse. Welche Restklassen kann man dividieren? Geben Sie ein Beispiel mit Probe.

37) Was besagt der *chinesische Restsatz*?  
Finden Sie alle ganzen Zahlen, die sowohl kongruent 2 modulo 11 als auch kongruent 4 modulo 9 sind. Gibt es drei verschiedene Lösungen?

38) Welche Zahlenwerte erhält man, wenn man im Datentyp

`unsigned int`

von C die Faktoriellen

$$n! \quad \text{für } n = 0, 1, 2, \dots$$

durch Multiplizieren berechnet? Welche Werte sind richtig, welche falsch?