Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

7. Exercise sheet
Hand in before Monday, 2005/12/19, 14^{00} in b-it 1.22.

Exercise 7.1 (u). (6+4 points)

For Dixon's random squares method B-smooth numbers were important. Denote by $\psi(x, B)$ the number of positive integers less than or equal to x whose prime divisors are at most B. Dickman's rho function $\varrho(x, B) = \psi(x, B)/x$ denotes the fraction of B-smooth integers.

(i) How many 2-smooth numbers are there up to 100? [This is $\psi(100, 2)$.] 1

(ii) How many 3-smooth numbers are there up to 100? [This is $\psi(100, 3)$.] 1

(iii) ... 10 000? [This is $\psi(10\,000, 3)$.] 1

In the course we used that $\varrho(x, b) \approx u^{-u}$ with $u = \ln(x)/\ln(B)$.

(iv) Compute the estimate xu^{-u} of 3-smooth numbers less than 10 000. Compare this to the exact value. 1

(v) How many 5-smooth numbers are there up to 10 000? [This is $\psi(10\,000, 5)$.] 1

(vi) Show how to calculate $\psi(x, p)$ with p prime from values $\psi(x/p^e, p-1)$. 1

(vii*) Write a (recursive) procedure `countsmooth(x,b)` that computes the exact number $\psi(x, b)$. (*Hint*: `numlib::prevprime(b)` might be helpful. Use `option remember` to save time. Remark: MuPAD has protected `psi` for the digamma function Γ'/Γ.) +2

Consider the value $B_x = \exp(\sqrt{\ln x \ln \ln x})$ that we derived for use in Dixon's random squares method.

(viii*) Plot the ratio $\varrho(x, B_x)/(u^{-u})$ for x in the range 1 through 10^6 with u calculated for $B = B_x$. +2