Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

3. Exercise sheet
Hand in before Monday, 2005/11/21, 14^{00} in b-it 1.22.

Exercise 3.1 (Euler totient function). (4+2 points)

In the course we defined the Euler totient function φ by $\varphi(N) = \#\mathbb{Z}_N^\times$, and we proved that $\varphi(p \cdot q) = (p-1)(q-1)$ if p and q are different primes.

(i) Compute $\varphi(5)$ and $\varphi(25)$. $\boxed{1}$

(ii) Compute $\varphi(p)$ for a prime p. $\boxed{1}$

(iii*) Compute $\varphi(p^e)$ for a prime p and some positive integer e. $\boxed{+1}$

(iv) Express $\varphi(a \cdot b)$ using $\varphi(a)$ and $\varphi(b)$ provided a and b are coprime, that is, they have no non-trivial common divisor. [Use the method from the course. Prove as a lemma that if a divides c and b divides c (and a, b are coprime) then ab divides c.] $\boxed{2}$

(v*) Suppose that the factorization of N is given: $N = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_r^{e_r}$ with pairwise different primes p_i and positive integers e_i. Give a formula for $\varphi(N)/N$. $\boxed{+1}$

Exercise 3.2 (Power of 3). (2 points)

Calculate $3^{1\,000\,003} \bmod 101$ by hand. *Hint*: You need almost no calculation for this!! $\boxed{2}$

Exercise 3.3 (Extrapolating . . .). (5 points)

(i) Assume that a factoring algorithm requires time $\Theta\left(\exp\left(\sqrt[2]{\ln N \ln\ln N}\right)\right)$ to find the prime factorization of a number N. And assume that this algorithm only needs a second to factorize a number less than 2^{100}. How large should N be so that this algorithm can not factorize N in less than the age of the universe, which is about $15 \cdot 10^9$ years or about 10^{18} seconds? $\boxed{3}$

(ii) How large should be a number if a new algorithm is found that requires only time $\Theta\left(\exp\left(2\sqrt[3]{\ln N (\ln\ln N)^2}\right)\right)$? $\boxed{1}$

(iii) How large should be a number if the new algorithm is optimized and now requires only time $\Theta\left(\exp\left(\sqrt[3]{\ln N (\ln\ln N)^2}\right)\right)$? $\boxed{1}$