Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 1

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, October 27th, at 12:05 pm.

1. Prove that the nth Fibonacci number F_n is divisible by 3 if and only if n is divisible by 4.

Hint. It helps to prove a more general statement about the repetition of remainders of Fibonacci numbers modulo 3 (with period 8).

2. The Euler phi function has the following properties (computational formulas):

(a) $\phi(p^k) = p^k - p^{k-1}$ for p prime and $k \in \mathbb{N}$;

(b) If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$;

(c) Let p_1, p_2, …, p_r be the distinct primes that divide n. Then

$$\phi(n) = n \cdot \Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big).$$

Prove (a) and (c). We will prove (b) together in the first exercise class.

3. Here ϕ is again Euler's phi function.

(a) Compute $\phi(1000000)$.

(b) Find all values of n that solve each of the following equations.

(i) $\phi(n) = n/2$;
(ii) $\phi(n) = n/3$;
(iii) $\phi(n) = n/6$.

4. Alice wants to construct her private key (p, q, d) and public key (n, e) for the RSA cryptosystem. She chooses $p = 5$ and $q = 7$. List all possible choices for pairs (e, d). Explain why your list is complete.