Topics in Algebra: Cryptography - Blatt 0

http://www.mat.univie.ac.at/~gagt/crypto2019

Goulnara Arzhantseva
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell
martin.finn-sell@univie.ac.at

This exercise sheet is intended to provide some warm up number theory questions that encourage us to think computationally. Terms to refresh yourself aree given in bold.

The following exercises are using **Euclid's algorithm** for computing **greatest common divisors**.

Question 1. Define the height $h(a)$ of a natural number $a \geq 2$ to be the greatest n such that Euclid's algorithm computes $\gcd(a, b)$ in n steps for some natural number $b < a$. Show that $h(a) = 1$ if and only if $a = 2$ and compute $h(a)$ for $a \leq 8$.

Question 2. The Fibonacci numbers $1, 1, 2, 3, 5, ...$ defined by $f_1 = f_2 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for all $n \geq 1$. Show that $0 < f_n < f_{n+1}$ for all $n > 1$. What happens if we apply Euclid's algorithm to a consecutive pair f_n, f_{n+1} of Fibonacci numbers? Show that $h(f_{n+2}) \geq n$.

The following exercises are about **primes numbers** and elementary **primality testing**.

Question 3. Suppose $p > 1$ and p divides $(p - 1)! + 1$. Then show p is prime.

Question 4. (Fermat) Show that if $2^m + 1$ is prime, then $m = 2^n$ for some natural number n.

Question 5. Describe the "Sieve of Erathosthenes" and use it to calculate all the primes $p \leq 100$.

The following are exercises that recall arithmetic in a finite fields and rings ($\mathbb{Z}_p$, where p is prime, or $\mathbb{Z}_n$, for any natural number n).

Question 6. State and prove **Fermat's little theorem**.

Question 7. (Wilson's Theorem) Show an integer n is prime if and only if $(n - 1)! \equiv -1 \mod n$.

Now we consider **Euler's Totient Function** ϕ

Question 8. Let $a, b \in \mathbb{N}$. Adapt your solution for question 6 to prove that if $\gcd(a, b) = 1$ then $a^{\phi(b)} \equiv 1 \mod b$.

Question 9. Compute $\phi(p^e)$ where p is prime and $e \geq 1$.

Question 10. Recall that an element $a \neq 0 \in \mathbb{Z}_n$ is a **primitive root** if multiplication by a in $\mathbb{Z}_n^\times$ has order $\phi(n)$. Show that if a is a primitive root, then $a^{k-l} \equiv 1 \mod n$ if and only if $k \equiv l \mod \phi(n)$.