Problem sheet 5
2018

Codierungstheorie und Kryptographie

26. (a) (Probably you did this one in a probability course): Let S be a set of q persons, randomly chosen from a large set of persons whose birthdays are uniformly independently distributed (u.i.d.) over the 365 days of a year. Determine the minimum number q such that the probability that there are at least two persons (among the q) having the same date as their birthday exceeds $p_1 = \frac{1}{2}$ or $p_2 = 0.999$. How does q change, if the concept of birthday is appropriately generalized, so that all persons have a u.i.d. label $b \in \{1, \ldots, N\}$, determine q as a function of N and p.

    (b) Fix $x \in \mathbb{Z}_N$, and randomly (u.i.d.) choose $r_1, \cdots, r_q \in \mathbb{Z}_N$. Show, when $q = \lfloor \sqrt{2N} \rfloor$ the probability that there exist i and j such that $r_i = x + r_j \bmod N$ is at least $p = 0.6$.

    (c) Let p be a prime, and let $g \in \mathbb{Z}_p^*$ be a primitive root. Show that one can find in $\mathbb{Z}_p^*$ the discrete logarithm of X to base g, if one can find r and s with $g^r = Xg^s \bmod p$. Use this and part b) to describe an algorithm which solves in $O(\sqrt{P})$ steps the discrete logarithm problem, with high probability.

27. Read about "birthday paradox attack". Apply it to signature schemes, where you want to persuade Alice to sign a document m, which she refuses to sign.

    Hint: create many essentially identical versions of m, (but with tiny changes, such as extra spaces), and also a quite different document M with many essentially identical versions that Alice would agree to sign.

    How does the underlying idea of the birthday paradox help you to forge Alice's signature on your preferred document m (or any of its versions)?

28. If the message m is long, (say a book of 500 pages!), and one performs any operation such as $m^a \bmod n$, then this is a quite long=expensive computation. Suggest how one can keep high security but reduce the costs. (There may be plenty of ideas, but also read about hash functions.)

29. (a) Determine for the primes $p = 5, 7, 11, 13, 17, 19$ the list of quadratic residues and nonresidues, (by hand or computer). Determine for these primes the least primitive root.

    (b) Find the smallest prime such that the least primitive root is larger than 10 (or 40). (Mathematica has a command "PrimitiveRootList", which certainly helps.)

30. (Not to be handed in): Have a brief look at https://eprint.iacr.org/2017/067

    Thorsten Kleinjung et al. manage to solve a dicrete logarithm problem over a prime field, where p has length 768 in binary. Also look at the state of the art on factoring RSA numbers (Wikipedia article on "RSA numbers". How many bits does the largest integer from that list have that has been factored?

    Based on this, what is the minimum/reasonable length of RSA or Discrete log problems that you could recommend?

31. (a) Search for information on "least primitive root" or least "non-square". There are different disciplines, such as a rigourous upper bound on the least primitive root for all primes, a conditional bound on assumptions such as the Riemann Hypothesis, a lower bound, in the sense, there exist infinitely many primes such that the least non-square is large, average over the primes, etc.

    (b) (Not to be handed in.) What does Artin's conjecture on primitive roots state? One is very far from proving it, but can show, with quite elementary methods, that for a positive proportion of all primes $p \leq y$ the number 2 generates at least $p^{\frac{1}{2}-\epsilon}$ many residue classes modulo p. Based on this (and numerical experiments), it has been conjectured that modulo most primes p one can write the residue class 0 in the form $1 + 2^i + 2^j \bmod p$.

    State of the art on this can be found in https://arxiv.org/abs/1602.05974 After lemma 2 there is a sketch proof of the statement above that the order of 2 modulo p is typically large.

32. Define a very simple primality test based on Wilson's criterion. Think about its computational complexity.

33. Define a primality test based on a refined version of Fermat's (little) theorem. (Hint: you can assume that a primitive root mudolo m exists iff $m = 1, 2, 4, p^e, 2p^e$, where p is an odd prime and $e \geq 1$. Assume that the factorization of $p - 1$ is known.)

34. (Compare with Einführung in die Algebra SS 2017)
    Let $G = \mathbb{Z}_{1729}^{\times}$, (where the "$\times$" means that only classes coprime to 1729 are used). Prove: for all $x \in G$: $x^{1728} \equiv 1 \bmod 1729$. Find $\exp G$, i.e. the smallest $t > 0$, such that for all $x \in G$: $x^t \equiv 1 \bmod 1729$. Find other composite numbers with this property. (There are many, you can find them with, but also (if you think a bit), without a computer).

35. Using quadratic reciprocity determine $(\frac{3}{p})$, depending on the congruence class of p mod 12.

36. a) Does $x^2 \equiv 17 \bmod 29$ have a solution?
    b) Does $x^2 \equiv 19 \bmod 30$ have a solution? (Chinese Remainder Theorem)

37. 1729 is the least number with two different representations as a sum of two cubes: $1729 = 1^3 + 12^3 = 9^3 + 10^3$, as famously observed by Ramanujan.

    Show that there is only one number n, namely 1729, which has the two properties: 1) $n = a^3 + b^3 = c^3 + d^3$ are two $d$istinct representations as a sum of two cubes
    2) n is a number of the form $n = (6k + 1)(12k + 1)(18k + 1)$, where all three factors are prime,

(nicht zum Ankreuzen) Write down some comments how the course could be improved in future years, (if you like anonymously, typed and with a cryptographic protocol which ensures complete anonymity).

To be handed in Tuesday 19th June.