Problem sheet 4
2020

Codierungstheorie und Kryptographie

20. (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.)

21. (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?

22. (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 almost all primes p one can write the residue class 0 in the form $1 + 2^i + 2^j \bmod p$.

    State of the art on partial results towards 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.

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

24. 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.)

25. (Miller-Rabin test) Work through the nice proof of the security level of the Miller-Rabin test in Johannes Buchmann, Einführung in die Kryptographie, `https://link.springer.com/book/10.1007%2F978-3-642-39775-2` In the tu-network you have free access to the German version.

    Theorem 7.6 Ist $n \geq 3$ eine ungerade zusammengesetzte Zahl, so gibt es in der Menge $\{1, \ldots, n-1\}$ höchstens $(n-1)/4$ Zahlen, die zu n teilerfremd und keine Zeugen gegen die Primalität von n sind. Based on this write a programme (any language or computer algebra package) that implements the Miller-Rabin test (say with $t = 10$ or 20 iterations), and find the smllest prime with 512 bits.

(In Mathematica the command `NextPrime`[2ˆ511] would give that prime, but this is obviously not what you are supposed to do. Do not use a built in command that tests primality, but you can use built in commands for gcd or congruence computations. For this you obviously need to work with a system that can deal with very large numbers, such as sage or mathematica. If this is a major problem, and you want to use C, python etc solve the corresponding problem with smaller primes.) Note: think about that modular exponentiaton like $151^{120000} \mod 101$ does not require to compute 151^{120000}, it is possible to keep all numbers very small.

Give for the final prime your analysis in which sense it is probably a prime, and give for at least some of the smaller numbers you tested a witness, why they are not prime.

26. (Compare with Einführung in die Algebra, in case you attended the course with me)
Let $G = \mathbb{Z}_{1729}^{\times}$, (where the "$\times$" means that only classes coprime to 1729 are used). Prove: for all $x \in G$: $x^{1728} \equiv 1 \mod 1729$. Find $\exp G$, i.e. the smallest $t > 0$, such that for all $x \in G$: $x^t \equiv 1 \mod 1729$. 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).

    In particular, prove property d) of Carmichael numbers in the lecture notes: For each prime divisor p of n one also has that $p-1$ divides $n-1$. Use this to contruct many integers (say products of three distinct prime numbers) which are Carmichael numbers.

27. Using quadratic reciprocity determine $(\frac{3}{p})$, depending on the congruence class of p mod 12.
Using quadratic reciprocity determine $(\frac{5}{p})$, depending on the congruence class of p mod 20.

28. a) Does $x^2 \equiv 17 \mod 29$ have a solution?
b) Does $x^2 \equiv 19 \mod 30$ have a solution? (Chinese Remainder Theorem)
c) Evaluate $(\frac{31}{103})$ and $(\frac{971}{15881})$.

29. (a) Let p be a prime, evaluate $\sum_{n=1}^{p}(\frac{n(n+1)}{p})$. (You can do some experiments for small primes, and then prove your observation.)
    (b) Assume that g_1 and g_2 are primitive roots modulo p. Investigate whether $g_1 g_2$ is always/sometimes/never a primitive root modulo p.

30. Let $N(p)$ denote the number of pairs of consecutive quadratic residues modulo p. Work out $N(p)$ and state a conjecture for a formula for $N(p)$. Try to prove it. (Part a) of the above problem can help.)

31. Calculate for $p = 31$ the $p \times p$ matrix with entry $a_{i,j} = (\frac{i+j}{p})$, $0 \leq i \leq p-1$ and $0 \leq j \leq p-1$. Let us study an $a \times b$ sub-structure, (let's call it sub-matrix) which is a the intersection of a set of a rows times with set of b columns. Search for the largest sub-matrix of (only) 1-entries. (at least 3×3). Show that there is a also a $a \times b$ sub-matrix of -1 entries.

    One can prove that $ab \leq p$. It is conjectured that in the symmetric case $a = b$ the maximum value of a should be much smaller than $\sqrt{p}$.

32. (not to handed in): work through the proof of quadratic reciprocity. Also observe that $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ follows from the version of the lecture notes.

To be handed in Wednesday, 3rd June 2020 (Kreuzesystem at 10.00, teach center a bit later).