Fall 2021 – Math 328K – 55385

Homework 11

due Tuesday, November 23, 14:00

Problem 1. Here is a way to construct a primitive root modulo p. Let the prime decomposition of $\phi(p) = p - 1$ be

$$p - 1 = q_1^{t_1} \cdots q_k^{t_k}$$

where $q_1, \ldots, q_k$ are distinct prime factors of $p - 1$.

a) Let $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $\operatorname{ord}(a)$ and $\operatorname{ord}(b)$ are coprime. Show that $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$.

b) Suppose that for each $i \in \{1, \ldots, k\}$ we have $a_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $\operatorname{ord}(a_i) = q_i^{t_i}$. We showed in class that such an integer exists (in fact, we proved there are $\phi(q_i^{t_i})$ of these). Show that then $a = a_1 \cdots a_k$ is a primitive root.

Problem 2. Alice tries a few improvements to Caesar's cipher ($c_i = m_i + k$). Find the keys using the frequencies of letters and decrypt the ciphertexts. The spaces are only there for readability, they don't correspond to spaces in the plain text.

E is by far the most frequent letter in the English language (11.2%), followed by A (8.5%), R (7.5%), I (7.5%), O (7.1%), T (7.0%), N (6.7%), S (5.7%) and L (5.5%).

a) The text is encrypted with a Caesar cipher, and then the result is encrypted again with Caesar cipher, using a different key.

FTUEU EQCGU HMXQZ FFAME UZSXQ OMQEM DOUBT QD

b) The cipher $c_i = am_i + b$, using two keys $a \in (\mathbb{Z}/26\mathbb{Z})^\times$ and $b \in \mathbb{Z}/26\mathbb{Z}$. *(This one is a bit more difficult. It might be helpful to use a computer.)*

FQKVF ZQQUL ZLSNI VFZVZ QUVSH BWVIJ MAJZZ LWKVT VXZ

c) The cipher $c_i = am_i + i$, using a key $a \in (\mathbb{Z}/26\mathbb{Z})^\times$ (the indices start with 0).

PMWJY LTDMF HVSXG NNBHE UILII FPBPE ECHZI TQLJF IUBBP

Problem 3. Two texts were encrypted with a Vigenère cipher, both using the same key. The ciphertexts are

We found out that the first message begins with HELLOBOB, and ends with ALICE, but we don't know what is in between.

ALLYY TUJRM ZKXAT BXAMP OIGKE LVRXS ZBCMH YNHLC VSIMV TVIX

AHVRK FOKZJ EKTR

Decrypt the second message.

Problem 4. Let $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive root. We want to show that either $[a]_{p^2}$ or $[a+p]_{p^2}$ is a primitive root in $\mathbb{Z}/p^2\mathbb{Z}$.

a) Let $n = \mathrm{ord}[a]_{p^2}$. Show that either $n = p(p-1)$ or $n = p-1$. The same holds for the order of $[a+p]_{p^2}$.

   Hint: Show that $n \mid p(p-1)$ *and* $p-1 \mid n$.

b) Show that at least one of $[a]_{p^2}$ and $[a+p]_{p^2}$ is not a solution of the equation $x^{p-1} = 1$, and is therefore a primitive root.