Math 25 Fall 2022

Problem Solving Exercise 4

Your name: _____

INSTRUCTIONS

You may begin the "exam" when ready.

Write your name in the space provided above.

Use of calculators is not permitted on the "exam". They are not likely to be of much help anyways.

Unless otherwise stated, you must justify your solutions to receive full credit. Work that is illegible may not be graded. Work that is scratched out will not be graded.

It is fine to leave you answer in a form such as $\ln(0.02)$ or $\sqrt{123412}$ or $(1341)^4(1231)^{-1}$. However, if an expression can be easily simplified (such as $e^{\ln(0.02)}$ or $\cos\pi$), you should simplify it.

This is not actually an exam!

The "exam" has been created with the intended length of 50 minutes. This midterm is collected at the end of the X-hour.

Good luck!

Long Answer Questions

(1) (10 points) The following ciphertext

36 04 04

was encrypted using the RSA public key ($e = 5, n = 51$). Find the plaintext associated to this message. Each block has size 2, there are no spaces. For convenience, the following table is provided:

x	1	2	3	4	5	6	7	8	9	10
$4^x \bmod 51$	4	16	13	1	4	16	13	1	4	16
$36^x \bmod 51$	36	21	42	33	15	30	9	18	36	21

Solution. First we find the private key. We do so by solving $ex = 5d \equiv 1 \pmod{\phi(51)}$. By multiplicativity $\phi(51) = \phi(3)\phi(17) = 32$. By inspection $d = 13$.

Via the table we see

$$4^{13} \equiv 4^{10}4^3 \equiv 4^2 \cdot 4^3 \equiv 4^5 \equiv 4 \pmod{51}.$$

Again using the table (note repeated entries)

$$36^{13} \equiv 21 \cdot 42 \equiv 15 \pmod{51}.$$

The message is 'ODD'. □

(2) (10 points) Let $N = 301 \cdot 97 + 2$. Compute $\left(\dfrac{N-261}{N+40}\right)$.

Solution. First, notice that $N+40 \equiv 1\cdot 3+2 \equiv 1 \pmod 4$ and $N+40 \equiv 1\cdot 5+2+0 \equiv 7 \pmod 8$. Next,

$$\begin{aligned}\left(\frac{N-261}{N+40}\right) &= \left(\frac{-301}{N+40}\right) = \left(\frac{-1}{N+40}\right)\left(\frac{N+40}{301}\right) = \left(\frac{-1}{N+40}\right)\left(\frac{42}{301}\right)\\ &= \left(\frac{-1}{N+40}\right)\left(\frac{42}{301}\right)\\ &= \left(\frac{-1}{N+40}\right)\left(\frac{2}{301}\right)\left(\frac{3}{301}\right)\left(\frac{7}{301}\right).\end{aligned}$$

By reciprocity for Jacobi symbols and supplements

$$= (1)\cdot(1)\cdot\left(\frac{301}{3}\right)\left(\frac{301}{7}\right) = \left(\frac{1}{3}\right)\left(\frac{301}{7}\right).$$

It turns out that $30+5\cdot(1) \equiv 0 \pmod 7$, so $7 \mid 301$. Therefore, the entire Jacobi symbol is 0. □

(3) (10 points) Consider the following function

$$g(n) := \sum_{\substack{p^e \,||\, n \\ p \text{ prime}}} \frac{p-1}{2} e$$

Show that when n is an odd positive integer, $n \equiv (-1)^{g(n)} \pmod 4$.

Solution. Let $n = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization; when n is odd, so are all the primes.

Notice for an odd integer n that $n \equiv (-1)^{\frac{n-1}{2}} \pmod 4$. Thus,

$$n \equiv \prod_{i=1}^{k} p_i^{e_i} \equiv \prod_{i=1}^{k} (-1)^{e_i \frac{p_i-1}{2}} \equiv (-1)^{\sum_{i=1}^{k} e_i \frac{p_i-1}{2}} \pmod 4.$$

Essentially by definition,

$$g(n) = \sum_{i=1}^{k} e_i \cdot \frac{p_i - 1}{2}.$$

□

(4) (10 points) Is the following statement true:

Theorem (?)**.** *Let p be an odd prime. Then the equation $x^2 \equiv 1 \pmod{p^e}$ has precisely two solutions for $x \in \mathbb{Z}/p^e\mathbb{Z}$.*

If the statement is true, provide a proof. If not, provide a counter-example.

Solution. The statement is indeed true. Pick a primitive element α mod p^e. Then

$$(\mathbb{Z}/p^e\mathbb{Z})^\times = \{1, \alpha, \ldots, \alpha^{\phi(p^e)-1}\}.$$

If $\alpha^{2j} \equiv 1 \pmod{p^e}$, then $\phi(p^e) \mid 2j$. Because $0 \leq j < \phi(p^e)$, we see $0 \leq 2j < 2\phi(p^e)$.

The only multiples of $\phi(p^e)$ in this interval are 0 and $\phi(p^e)$. That is, the only solutions to $\alpha^{2j} \equiv 1 \pmod{p^e}$ are $j = 0, \dfrac{\phi(p^e)}{2}$. □

(5*) (4 points) Let $a_0, \ldots, a_k \in \mathbb{Z}/p\mathbb{Z}$ and let $0 \leq k < p$. Show that there exists a polynomial $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ of degree at most k such that $f(x)$ satisfies the system of congruences

$$\begin{aligned} f(x) &\equiv a_0 \pmod{x} \\ &\cdots \\ f(x) &\equiv a_k \pmod{x-k} \end{aligned}$$

One can think of this as a Chinese Remainder Theorem for polynomials.

Solution. Recall from the division algorithm for polynomials that for any $\alpha \in \mathbb{Z}/p\mathbb{Z}$,

$$f(x) = g(x)(x-\alpha) + f(\alpha).$$

We consider the polynomials

$$N(x) = \prod_{i=0}^{k-1}(x-i), \quad \hat{N}_i(x) = \frac{N(x)}{x-i}.$$

Observe that $\hat{N}_i(x) \pmod{x-i} = \hat{N}_i(i) \not\equiv 0 \pmod{p}$, since $0, \ldots, k$ are in distinct residue classes modulo p by assumption. In particular, there are solutions $c_i \in \mathbb{Z}/p\mathbb{Z}$ to the congruences

$$\hat{N}_i(i) \cdot c_i \equiv 1 \pmod{p}.$$

We now finally construct the polynomial. We set

$$F(x) = \sum_{j=0}^{k} c_j \cdot \hat{N}_j(x) \cdot a_j.$$

By construction, we have that $\hat{N}_i(j) = 0$ unless $i = j$. Thus

$$F(i) = c_i \hat{N}_i(i) \cdot a_i = a_i \quad (\text{in } \mathbb{Z}/p\mathbb{Z}).$$

Furthermore, each $\hat{N}_i(x)$ has degree k, so $F(x)$ has degree at most k, as desired. $\square$

(6**) Let M be a set of 1985 positive integers, none of which has a prime factor larger than 23. Prove that there exists a subset of M with four elements whose product is a perfect 4-th power.

Solution. For entertainment purposes, the solutions have not been included. □

(This page is intentionally left blank in case you need extra space for any of the problems. **If you use this page for a particular problem, it is essential that you make a note on the page where the problem appears, indicating that your work is continued here.)**