Math 25 Fall 2022

Problem Solving Exercise 2

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

$$32\ 15\ 32$$

was encrypted using the RSA public key ($e = 5, \mathbf{n = 35}$). 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	4	8	16
15^x	mod	35	15	15	15	15	15
32^x	mod	35	32	9	11	16	11

Solution. First we find the private key. We do so by solving $ex = 5d \equiv 1 \pmod{\phi(35)}$. By multiplicativity $\phi(35) = \phi(5)\phi(7) = 24$. By inspection $d = 5$.

Via the table we see

$$15^5 \equiv 15^{4+1} \equiv 15 \cdot 15 \equiv 15^2 \equiv 15 \pmod{35}.$$

One can be clever and notice that $2^5 = 32$. Alternatively, using the table,

$$32^5 \equiv 32^4 \cdot 32 \equiv 11 \cdot 32 \equiv (320 + 32) \equiv 352 \equiv 2 \pmod{35}.$$

In any case the message is 'BOB'. □

(2) (10 points) The *Fibonnaci numbers* are defined recursively by the formula $f_1 = 1, f_2 = 1$, and

$$f_{n+2} = f_{n+1} + f_n, \quad n \geq 1.$$

For example, the first few Fibonacci numbers are $1, 1, 2, 3, 5, 8, 13, \ldots$.

Prove that consecutive Fibonacci numbers are coprime.

Solution. We proceed by induction. The base case $\gcd(f_1, f_2) = 1$ is clear. We assume for the sake of induction that $\gcd(f_n, f_{n+1}) = 1$. Then by Bezout we may find integers x, y so that

$$xf_n + yf_{n+1} = 1.$$

But $f_{n+2} - f_{n+1} = f_n$, so

$$x(f_{n+2} - f_{n+1}) + yf_{n+1} = xf_{n+2} + (y - x)f_{n+1} = 1.$$

In other words, $\gcd(f_{n+1}, f_{n+2}) \mid 1$, i.e., it *is* 1. This shows the result for n implies the result for $n + 1$, and by induction the result is true in general. □

(3) (10 points) Let n be an integer with prime factorization $p_1^{e_1} \dots p_k^{e_k}$ and let $a \in \mathbb{Z}/n\mathbb{Z}$. Prove that a is a square modulo n if and only if each $a \pmod{p_i^{e_i}}$ is a square.

Solution. ($\Rightarrow$) If $a \equiv x^2 \pmod{n}$, then we reduce this equation modulo $p_i^{e_i}$ to see $a \equiv x^2 \pmod{p_i^{e_i}}$. That is, a is a square modulo each prime power.

($\Leftarrow$) Write $a \equiv x_i^2 \pmod{p_i^{e_i}}$ for each i. By the CRT, we see that there exists an $x \pmod{n}$ such that $x \equiv x_i \pmod{p_i^{e_i}}$ for each i. Now

$$x^2 \equiv x_i^2 \equiv a \pmod{p_i^{e_i}}$$

for each i. By *uniqueness* in the Chinese Remainder Theorem, we have $x^2 \equiv a \pmod{n}$. Thus a is a square. $\square$

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

Theorem (?)**.** *Let p be an odd prime and let k be a positive integer such that $p-1 \nmid k$. Then*

$$\sum_{a=0}^{p-1} a^k \equiv 0 \pmod{p}.$$

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

Solution. The statement is indeed true. Let α be a primitive element modulo p. Then

$$\sum_{a=0}^{p-1} a^k = 0^k + \sum_{a=1}^{p-1} a^k = \sum_{j=0}^{p-2} (\alpha^j)^k$$

because powers of α enumerate all of the elements of $\mathbb{Z}/p\mathbb{Z}^\times$. Because $p-1 \nmid k$, we have that $\alpha^k \not\equiv 1 \pmod{p}$ because it is a primitive element. (We have $\alpha^e \equiv 1 \pmod{p}$ if and only if the order of α divides e, from Lagrange.)

Thus, we have

$$\sum_{j=0}^{p-2} (\alpha^j)^k \equiv \frac{\alpha^{k(p-1)} - 1}{\alpha^k - 1} \pmod{p}$$

and the denominator is a unit, so the expression is well-defined. (Dividing is the same as multiplying by the inverse, provided the inverse exists.) By Fermat's little theorem the numerator is zero modulo p, and the claim is proven.

Remark: The indexing of the sum is slightly different than the solution I gave earlier. Both are valid approaches. □

(5*) (4 points) A polynomial $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ is *irreducible* if any factorization $f(x) = a(x)b(x)$ has either $\deg a(x) = 0$ or $\deg b(x) = 0$. Prove that any non-zero polynomial $f(x) \neq 0$ admits a factorization

$$f(x) = \prod_{i=1}^{k} p_i(x)^{e_i}$$

where each $p_i(x)$ is irreducible and each $e_i \geq 1$ is an integer. (You *do not* need to show the factorization is unique.)

Solution. We proceed by induction on the degree. For polynomials of degree 0, any factorization $f(x) = a(x)b(x)$ has both $\deg a(x) = \deg b(x) = 0$, since p is prime (see a previous homework).

We assume the result for all degrees up to some $d \geq 0$ and show this implies the degree $d+1$ case. Let $f(x)$ be a polynomial of degree $d+1$. If $f(x)$ is irreducible, then $f(x) = f(x)^1$ is an irreducible factorization. Otherwise, $f(x)$ is reducible, so we write $f(x) = a(x)b(x)$ for some $a(x), b(x)$ of positive degree. Because $\deg f(x) = \deg a(x) + \deg b(x)$, we have that $\deg a(x), \deg b(x) \leq d$. In other words, by the induction hypothesis,

$$f(x) = a(x)b(x) = \prod_{i=1}^{k} p_i(x)^{e_i} \cdot \prod_{i=1}^{\ell} q_i(x)^{e_i}$$

i.e., $f(x)$ admits a factorization into irreducibles, as claimed. By induction we are done. $\square$

(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.)**