MATH 233: ASSIGNMENT 4

DUE: FRIDAY, FEBRUARY 23, 11:59PM ON GRADESCOPE
UNIVERSITY OF ROCHESTER, SPRING 2024

Problem 1. (a) (5.4.2) The LFSR sequence 10011101 ... is generated by a recurrence relation of length 3: $x_{n+3} \equiv c_0 x_n + c_1 x_{n+1} + c_2 x_{n+2} \pmod 2$. Find the coefficients c_0, c_1, c_2.

(b) (5.4.8) Suppose we build an LFSR-type machine that works mod 2. It uses a recurrence of length 2 of the form $x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} + 1 \pmod 2$ to generate the sequence 11001100 .... Find c_0 and c_1.

Problem 2. (a) (3.13.16) Find x with $x \equiv 3 \pmod 5$ and $x \equiv 9 \pmod{11}$.

(b) (3.13.17) Find x with $2x \equiv 1 \pmod 7$ and $4x \equiv 2 \pmod 9$. (*Hint*: Replace $2x \equiv 1 \pmod 7$ with $x \equiv a \pmod 7$ for a suitable a, and similarly for the second congruence.)

Problem 3 (3.13.21)**.** (a) Find all four solutions to $x^2 \equiv 133 \pmod{143}$. (Note that $143 = 11 \cdot 13$.)

(b) Find all solutions to $x^2 \equiv 77 \pmod{143}$. (There are only two solutions in this case. This is because $\gcd(77, 143) \neq 1$. You may need to use 3.13.14(a).)

Problem 4 (3.13.42)**.** (a) Use the Legendre symbol to show that $x^2 \equiv 5 \pmod{19}$ has a solution.

(b) Find all solutions to $x^2 \equiv 5 \pmod{19}$. (There are two solutions. Do NOT use the brute-force search.)

Problem 5. (a) (3.13.25) Find the last 2 digits of 123^{562}. (*Hint*: Use mod 100.)

(b) Find the last 7 digits of the binary representation of 123^{643}. (*Hint*: $2^6 = 64$ and $2^7 = 128$.)

Problem 6 (3.13.53)**.** Let a and $n > 1$ be integers with $\gcd(a, n) = 1$. The **order** of a mod n is the smallest positive integer r such that $a^r \equiv 1 \pmod n$. We denote $r = \mathrm{ord}_n(a)$.

(a) Show that $r \leq \phi(n)$.

(b) Show that if $m = rk$ is a multiple of r, then $a^m \equiv 1 \pmod n$.

(c) Suppose $a^t \equiv 1 \pmod n$. Write $t = qr + s$ with $0 \leq s < r$ (this is just division with remainder). Show that $a^s \equiv 1 \pmod n$. Then using the definition of r and the fact that $0 \leq s < r$, show that $s = 0$ and therefore $r \mid t$, i.e., r divides t. (This, combined with part (b), yields the result that $a^t \equiv 1 \pmod n$ if and only if $\mathrm{ord}_n(a) \mid t$.)

(d) Show that $\mathrm{ord}_n(a) \mid \phi(n)$.