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: $x_{n+3} \equiv c_0x_n + c_1x_{n+1} + c_2x_{n+2} \pmod 2$. 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 $x_{n+2} \equiv c_0x_n + c_1x_{n+1} + 1 \pmod 2$ to generate the sequence 11001100 . . .. Find c_0 and c_1.

Solution. (a) We construct a matrix (modular) equation as

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 1\end{pmatrix}\begin{pmatrix}c_0\\ c_1\\ c_2\end{pmatrix} \equiv \begin{pmatrix}1\\ 1\\ 1\end{pmatrix} \pmod 2.$$

The matrix is invertible with inverse

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 1 & 0\end{pmatrix}$$

mod 2, so

$$\begin{pmatrix}c_0\\ c_1\\ c_2\end{pmatrix} \equiv \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 1\\ 1\end{pmatrix} \equiv \begin{pmatrix}1\\ 0\\ 1\end{pmatrix} \quad \Rightarrow \quad (c_0, c_1, c_2) \equiv (1, 0, 1) \pmod 2.$$

The recurrence relation $x_{n+3} \equiv x_n + x_{n+2} \pmod 2$ generates the given sequence well.

(b) We first construct a system of linear (modular) equations (mod 2) as

$$\begin{aligned} c_0 + c_1 + 1 &\equiv 0,\\ c_0 \qquad + 1 &\equiv 0. \end{aligned}$$

Now we represent this with a matrix equation:

$$\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}c_0\\ c_1\end{pmatrix} + \begin{pmatrix}1\\ 1\end{pmatrix} \equiv \begin{pmatrix}0\\ 0\end{pmatrix} \pmod 2 \quad \Rightarrow \quad \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}c_0\\ c_1\end{pmatrix} \equiv \begin{pmatrix}1\\ 1\end{pmatrix} \pmod 2.$$

The matrix is invertible with inverse

$$\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$$

mod 2, so

$$\begin{pmatrix}c_0\\ c_1\end{pmatrix} \equiv \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix} \equiv \begin{pmatrix}1\\ 0\end{pmatrix} \quad \Rightarrow \quad (c_0, c_1) \equiv (1, 0) \pmod 2.$$

The recurrence relation $x_{n+2} \equiv x_n + 1 \pmod 2$ generates the given sequence well.

□

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.)

Solution. (a) $5 \cdot (-2) + 11 \cdot 1 = 1$, so

$$x \equiv 9 \cdot 5 \cdot (-2) + 3 \cdot 11 \cdot 1 \equiv -57 \equiv 53 \pmod{55}.$$

(b) We have

$$2^{-1} \equiv 4 \pmod 7 \quad \Rightarrow \quad x \equiv 4 \pmod 7,$$

and

$$4^{-1} \equiv 7 \pmod 9 \quad \Rightarrow \quad x \equiv 2 \cdot 7 \equiv 5 \pmod 9.$$

Then $7 \cdot 4 + 9 \cdot (-3) = 1$, so

$$x \equiv 5 \cdot 7 \cdot 4 + 4 \cdot 9 \cdot (-3) \equiv 32 \pmod{63}.$$

□

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).)

Solution. (a) We have

$$x^2 \equiv 133 \equiv 1 \pmod{11} \quad \Rightarrow \quad x \equiv \pm 1 \pmod{11}.$$

On the other hand,

$$x^2 \equiv 133 \equiv 3 \pmod{13} \quad \Rightarrow \quad x \equiv \pm 4 \pmod{13}$$

obtained by an exhaustive search. (Since $13 \not\equiv 3 \pmod 4$, you cannot use the method introduced in the lecture.) Applying CRT to each of four pairs using $11 \cdot 6 + 13 \cdot (-5) = 1$, we have

$$\begin{aligned}
x \equiv 1 \pmod{11}, \quad x \equiv 4 \pmod{13} \quad &\Rightarrow \quad x \equiv 4 \cdot 11 \cdot 6 + 1 \cdot 13 \cdot (-5) \\
&\qquad \equiv 199 \equiv 56 \pmod{143}, \\
x \equiv 1 \pmod{11}, \quad x \equiv -4 \pmod{13} \quad &\Rightarrow \quad x \equiv (-4) \cdot 11 \cdot 6 + 1 \cdot 13 \cdot (-5) \\
&\qquad \equiv -329 \equiv 100 \pmod{143}, \\
x \equiv -1 \pmod{11}, \quad x \equiv 4 \pmod{13} \quad &\Rightarrow \quad x \equiv (4) \cdot 11 \cdot 6 + (-1) \cdot 13 \cdot (-5) \\
&\qquad \equiv 329 \equiv 43 \pmod{143}, \\
x \equiv -1 \pmod{11}, \quad x \equiv -4 \pmod{13} \quad &\Rightarrow \quad x \equiv (-4) \cdot 11 \cdot 6 + (-1) \cdot 13 \cdot (-5) \\
&\qquad \equiv -199 \equiv 87 \pmod{143}.
\end{aligned}$$

(b) We have

$$x^2 \equiv 77 \equiv 0 \pmod{11} \quad \Rightarrow \quad x \equiv 0 \pmod{11}$$

from 3.13.14(a). On the other hand,

$$x^2 \equiv 77 \equiv 12 \pmod{13} \quad \Rightarrow \quad x \equiv \pm 5 \pmod{13}$$

obtained by an exhaustive search. Applying CRT to each pair, we have

$$\begin{aligned} x \equiv 0 \pmod{11}, \quad x \equiv 5 \pmod{13} \quad &\Rightarrow \quad x \equiv 5 \cdot 11 \cdot 6 + 0 \cdot 13 \cdot (-5) \\ &\qquad\quad \equiv 330 \equiv 44 \pmod{143}, \\ x \equiv 0 \pmod{11}, \quad x \equiv -5 \pmod{13} \quad &\Rightarrow \quad x \equiv (-5) \cdot 11 \cdot 6 + 0 \cdot 13 \cdot (-5) \\ &\qquad\quad \equiv -330 \equiv 99 \pmod{143}. \end{aligned}$$

□

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.)

Solution. (a) Note that the Legendre symbol also satisfies the law of quadratic reciprocity. Therefore,

$$\begin{aligned} \left(\frac{5}{19}\right) &= \left(\frac{19}{5}\right) \qquad (5 \equiv 1 \pmod{4}) \\ &= \left(\frac{4}{5}\right) \\ &= 1, \end{aligned}$$

since $x^2 \equiv 4 \pmod{5}$ has solutions $x \equiv \pm 2 \pmod{5}$. Therefore, $x^2 \equiv 5 \pmod{19}$ also has a solution.

(b) Since $19 \equiv 3 \pmod{4}$, we consider

$$5^{(19+1)/4} \equiv 5^5 \equiv 9 \pmod{19}.$$

Since

$$9^2 \equiv 81 \equiv 5 \pmod{19},$$

we can conclude that the solutions to $x^2 \equiv 5 \pmod{19}$ are

$$x \equiv \pm 9 \pmod{19}.$$

□

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 $2^7 = 128$.)

Solution. (a) Since $100 = 2^2 \cdot 5^2$,

$$\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40 \quad \Rightarrow \quad 123^{40} \equiv 1 \pmod{100}$$

by Euler's theorem. (Note that $\gcd(100, 123) = 1$.) Therefore, since $562 \equiv 2 \pmod{40}$, we have

$$123^{562} \equiv 123^2 \equiv 23^2 \equiv 29 \pmod{100},$$

so the last 2 digits of 123^{562} are 29.

(b) We need to use mod $2^7 = 128$. Since $\gcd(128, 123) = 1$ and

$$\phi(128) = 128\left(1 - \frac{1}{2}\right) = 64 \quad \Rightarrow \quad 123^{64} \equiv 1 \pmod{128}$$

by Euler's theorem, we have

$$123^{643} \equiv 123^3 \equiv (-5)^3 \equiv -125 \equiv 3 \pmod{128}.$$

This implies that the last 7 digits of the binary representation of 123^{643} are 0000011.

□

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

Solution. (a) $a^{\phi(n)} \equiv 1 \pmod{n}$ by Euler's theorem. Therefore, $r \leq \phi(n)$ from the definition of r.

(b) We have

$$a^m \equiv a^{rk} \equiv (a^r)^k \equiv 1 \pmod{n}.$$

(c) We have

$$1 \equiv a^t \equiv a^{qr+s} \equiv a^{qr}a^s \equiv (a^r)^q a^s \equiv a^s \pmod{n}.$$

$s > 0$ contradicts the definition of r, so $s = 0$ and $r \mid t$.

(d) Since $a^{\phi(n)} \equiv 1 \pmod{n}$, $r = \mathrm{ord}_n(a)$ should divide $\phi(n)$ by part (c).

□