CSCI 104 **Homework 6** Hanting Zhang

Problem 1. Use the recursive pattern $x_{n+1} = (ax_n + c) \bmod m$ to generate the first 5 pseudorandom numbers $x_1, x_2, \dots, x_5$ is the sequence given $a = 13, c = 7, x_0 = -5, m = 12$.

Note that $x_{n+1} = 13x_n + 7 \bmod 12 = x_n + 7 \bmod 12$. Then just compute:

$$\begin{aligned}
x_1 &= x_0 + 7 \bmod 12 = -5 + 7 \bmod 12 = 2 \\
x_2 &= x_1 + 7 \bmod 12 = 9 \\
x_3 &= x_2 + 7 \bmod 12 = 4 \\
x_4 &= x_3 + 7 \bmod 12 = 11 \\
x_5 &= x_4 + 7 \bmod 12 = 6
\end{aligned}$$

Problem 2. How many zeros are at the end of 100!?

The number of zeros is equal to the number of factors of 10 in 100!. Every factor of 10 is made from exactly one factor of 2 and 5. Since there are more factors of 2 than factors of 5, the number of zeros is equal to the number of factors of 5. There are

$$\left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor = 20 + 4 = 24$$

factors of 5, hence there are 24 zeros at the end of 100!.

Problem 3. Prove that for any integer n, $n^5 - 5n^3 + 4n$ is divisible by 5.

Proof. The term $-5n^3$ is always divisble by 5, so it suffices to prove that $n^5 - 4n$ is divisible by 5. Note that Fermat's Little Theorem, $n^4 \equiv 1 \bmod 5$ for any n. Thus

$$n^5 + 4n \equiv n(n^4 + 4) \equiv n(1 + 4) \equiv 5n \equiv 0 \bmod 5,$$

which is what we want. Hence $n^5 - 5n^3 + 4n$ is divisible by 5 for any n, as desired. □

Problem 4. Compute $1333^{42} \bmod 11$.

Note $11^3 = 1331$ so $1333 \equiv 2 \bmod 11$. Then $\varphi(11) = 10$, so

$$1333^{42} \equiv 2^{42} \equiv (2^{10})^4(2^2) \equiv 1^4 \cdot 2^2 \equiv 4 \bmod 11.$$

Problem 5. Two integers $x, y \in \mathbb{Z}$ are said to be relatively prime if their greatest common divisor is 1. Use (and show the steps to) the Euclidean algorithm to determine if 309 and 112 are relatively prime.

Just compute:

$$\begin{aligned}
309 &= 2(112) + 85 \\
112 &= 1(85) + 27 \\
85 &= 3(27) + 4 \\
27 &= 6(4) + 3 \\
4 &= 1(3) + 1 \\
3 &= 3(1).
\end{aligned}$$

Hence $\gcd(309, 112) = 1$ and 309 and 112 are relatively prime.

Problem 6. Solve $54x + 16y = \gcd(54, 16)$. Show your work in such a way that allows the grader to recognize that you understand the relevant lecture material.

Just compute:

$$\begin{aligned}
54 &= 3(16) + 6 \\
16 &= 2(6) + 4 \\
6 &= 1(4) + 2 \\
4 &= 2(2).
\end{aligned}$$

Hence $\gcd(54, 16) = 2$. Now to find x and y:

$$\begin{aligned}
2 &= 6 - 1(4) \\
2 &= 6 - (16 - 2(6)) = 3(6) - 16 \\
2 &= 3(54 - 3(16)) - 16 = 3(54) - 9(16) - 16 = 3(54) - 10(16) \\
&\Rightarrow x = 3, y = 10.
\end{aligned}$$

Problem 7. Find the multiplicative inverse of $x \equiv 33 \bmod 112$.

We want to solve $33x + 112y = 1$. Just compute:

$$\begin{aligned}
112 &= 3(33) + 13 \\
33 &= 2(13) + 7 \\
13 &= 1(7) + 6
\end{aligned}$$

$$\begin{aligned} 7 &= 1(6) + 1 \\ 6 &= 6(1). \end{aligned}$$

Hence $\gcd(112, 33) = 1$. Now find x and y:

$$\begin{aligned} 1 &= 7 - 1(6) \\ &= 7 - 1(13 - 1(7)) = 2(7) - 13 \\ &= 2(33 - 2(13)) - 13 = 2(33) - 5(13) \\ &= 2(33) - 5(112 - 3(33)) = 17(33) - 5(112) \\ &\Rightarrow x = 17, y = -5. \end{aligned}$$

So 17 is the inverse of 33.