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

$$x_1 = (13 \cdot (-5) + 7) \% 12 = -58 \% 12 = \underline{2}$$
$$x_2 = (13 \cdot (2) + 7) \% 12 = 33 \% 12 = \underline{9}$$
$$x_3 = (13 \cdot (9) + 7) \% 12 = 124 \% 12 = \underline{4}$$
$$x_4 = (13 \cdot (4) + 7) \% 12 = 59 \% 12 = \underline{11}$$
$$x_5 = (13 \cdot (11) + 7) \% 12 = 150 \% 12 = \underline{6}$$

$$\boxed{x_1 = 2, \; x_2 = 9, \; x_3 = 4, \; x_4 = 11, \; x_5 = 6}$$

2) How many zeros are at the end of 100!

$100 \cdot 99 \cdot 98 \cdot 96 \cdot 95 \cdot 94 \cdot 93 \cdot 92 \cdot 91 \cdot 90$

0 0 0

x 99

multiples of 5 are more than 2 so they take precedence

20 terms divisible by 5 in 100! {5, 10, 15, ... 95, 100}

4 terms divisible by 25 {25, 50, 75, 100}

20 terms + 4 terms also multiple factors of 5
100! factorial yields a total of 20+4 = 24 zeroes at the end

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

$\underbrace{\text{2 cases: either odd or even integer}}_{\text{possible way to solve}}$

$$n^5-5n^3+4n$$

$$n(n^4-5n^2+4)$$

$$\underset{3}{n}\underset{5}{(n-2)}\underset{1}{(n+2)}\underset{4}{(n-1)}\underset{2}{(n+1)}$$

$(n+2)(n+1)(n)(n-1)(n-2)$

at least 1 must be divisible by 5 since they're 5 consecutive integers. Because they are all being multiplied, that one number makes the equation is divisible by 5.

A) Compute $1333^{42} \bmod 11$

$$
\begin{array}{r}
121 \\
11 \overline{)1333} \\
-11 \\
\hline
23 \\
-22 \\
\hline
13 \\
-11 \\
\hline
2 = r
\end{array}
$$

$r = 2$

Fermat's theorem

$a^{p-1} \equiv 1 \pmod p$

$\equiv (1333^{42}) \bmod 11$

$= (1333^{10} \cdot 1333^{10} \cdot 1333^{10} \cdot 1333^{10} \cdot 1333^{2}) \bmod 11$

$\overset{FT}{\equiv} (1 \cdot 1 \cdot 1 \cdot 1 \cdot 2^2) \bmod 11$

$\equiv 2^2 \bmod 11$

$\boxed{1333^{42} \bmod 11 \equiv 4}$

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.

if $\gcd(a,b)=1$, they are relatively prime

$$309 = 2 \cdot 112 + 85$$
$$112 = 1 \cdot 85 + 27$$
$$85 = 3 \cdot 27 + 4$$
$$27 = 6 \cdot 4 + 1$$
$$4 = 4 \cdot 1 + 0$$
$$\gcd(309, 112) = 1$$

$\boxed{\text{Since the } \gcd(309,112)=1\text{, we can conclude 309 and 112 are relatively prime.}}$

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

$$54 = 16 \cdot 3 + 6 \qquad 6 = 54 - 16 \cdot 3$$

$$16 = 2 \cdot 6 + 4 \qquad 4 = 16 - 2 \cdot 6$$

$$6 = 1 \cdot 4 + 2 \qquad 2 = 6 - 1 \cdot 4$$

$$4 = 2 \cdot 2 + 0$$

$$\gcd(54, 16) = 2 \qquad r0 = 54, r1 = 16$$

$$6 = r0 - 3r1$$

$$4 = 16 - (2 \cdot 6)$$

$$4 = 16 - (2r0 - 6r1)$$

$$2 = r0 - 3r1 - 1(16 - 2r0 + 6r1)$$

$$2 = r0 - 3r1 - \underbrace{16}_{=r1} + 2r0 - 6r1$$

$$2 = r0 - 4r1 + 2r0 - 6r1$$

$$2 = 3r0 - 10r1$$

$$2 = 3 \cdot 54 - 10 \cdot 16$$

$$\boxed{x = 3, y = -10}$$

7) Find the multiplicative inverse of $x = 33 \bmod 112$

$y \cdot x \equiv 1 \bmod 112$

$33y \equiv 1 \bmod 112$

$\gcd(112, 33) = 112 = 3 \cdot 33 + 13$

$33 = 13 \cdot 2 + 7$

$\gcd(33, 112) \equiv 112x + 33y$

$r0 = 112, r1 = 33$

$13 = 1 \cdot 7 + 6$

$7 = 6 \cdot 1 + 1$

$6 = \underbrace{1}\cdot 6 + 0$

$\underbrace{\gcd(112, 33) = 1}_{\text{exists}}$

$1 = 7 - (6 \cdot 1)$

$6 = 13 - (7 \cdot 1)$

$1 = 7 - (13 - 7)$

$1 = 2 \cdot 7 - 13$

$7 = 33 - 13 \cdot 2$

$1 = 2 \cdot 33 - 5 \cdot 13$

$13 = 112 - 33 \cdot 3$

$1 = 2 \cdot 33 - 5(112 - 33 \cdot 3)$

$1 = 2 \cdot 33 - 5 \cdot 112 + 15 \cdot 33$

$1 = \underbrace{17} \cdot 33 - 5 \cdot 112$

$\boxed{\text{$y = 17$ is the multiplicative inverse of $x = 33 \bmod 112$}}$