ASSIGNMENT #10 SOLUTIONS

1: $5 \equiv 5 \bmod 13$, $5 \cdot 2 = 10 \equiv 10 \bmod 13$

$5 \cdot 2^2 \equiv 10 \cdot 2 \bmod 13$
$\equiv 20 \bmod 13$
$\equiv 7 \bmod 13$

$5 \cdot 2^3 \equiv 7 \cdot 2 \bmod 13$
$\equiv 14 \bmod 13$
$\equiv 1 \bmod 13$

$5 \cdot 2^4 \equiv 1 \cdot 2 \bmod 13$
$\equiv 2 \bmod 13$

$5 \cdot 2^5 \equiv 2 \cdot 2 \bmod 13$
$\equiv 4 \bmod 13$

$\Longrightarrow \boxed{5, 10, 7, 1, 2, 4}$

2: MULTIPLES OF 17: $-51, -34, -17, 0, 17, 34, 51$

$4 \equiv 4 \bmod 17$

$4 \cdot 10 = 40 \equiv 6 \bmod 17$

$4 \cdot 10^2 \equiv 6 \cdot 10 \bmod 17$
$\equiv 60 \bmod 17$
$\equiv 9 \bmod 17$

$4 \cdot 10^3 \equiv 9 \cdot 10 \bmod 17$
$\equiv -8 \cdot -7 \bmod 17$
$\equiv 56 \bmod 17$
$\equiv 5 \bmod 17$

$4 \cdot 10^4 \equiv 5 \cdot 10 \bmod 17$
$\equiv 50 \bmod 17$
$\equiv 16 \bmod 17$

$4 \cdot 10^5 \equiv 16 \cdot 10 \bmod 17$
$\equiv -1 \cdot -7 \bmod 17$
$\equiv 7 \bmod 17$

$\Longrightarrow \boxed{4, 6, 9, 5, 16, 7}$

$10^2 = 25 \equiv 10 \bmod 15$, SO FOR ANY $a \in \mathbb{N}$ $10^a \equiv 10 \bmod 15$

$7 \equiv 7 \bmod 15$ $\quad$ $7 \cdot 10 = 70 = 10 + 60$
$\equiv 10 \bmod 15$

SO FOR ALL ALL $a \in \mathbb{N}$, $7 \cdot 10^a \equiv 7 \cdot 10 \bmod 15$
$\equiv 10 \bmod 15$

$\Longrightarrow \boxed{7, 10, 10, 10, 10, 10}$

MULTIPLES OF 23: $-92, -69, -46, -23, 0, 23, 46, 69, 92$

$3 \equiv 3 \bmod 23$

$3 \cdot 11 = 33 \equiv 10 \bmod 23$

$3 \cdot 11^2 \equiv 10 \cdot 11 \bmod 23$
$\equiv 110 \bmod 23$
$\equiv 18 \bmod 23$

$3 \cdot 11^3 \equiv 18 \cdot 11 \bmod 23$
$\equiv -5 \cdot 11 \bmod 23$
$\equiv -55 \bmod 23$
$\equiv 14 \bmod 23$

$3 \cdot 11^4 \equiv 14 \cdot 11 \bmod 23$
$\equiv -9 \cdot 11 \bmod 23$
$\equiv -99 \bmod 23$
$\equiv -7 \bmod 23$
$\equiv 16 \bmod 23$

$3 \cdot 11^5 \equiv 16 \cdot 11 \bmod 23$
$\equiv -7 \cdot 11 \bmod 23$
$\equiv -77 \bmod 23$
$\equiv -8 \bmod 23$
$\equiv 15 \bmod 23$

$\Longrightarrow \boxed{3, 10, 18, 14, 16, 15}$

MULTIPLES OF 137: $-548, -411, -274, -137, 0, 137, 274, 411, 548$

$8 \equiv 8 \bmod 137$ $\quad 8 \cdot 13 = 104 \equiv 104 \bmod 137$

NOTE $548 \cdot 2 = 1096$ ALSO A MULTIPLE OF 137

$$\begin{aligned}
8 \cdot 13^2 &\equiv 104 \cdot 13 \bmod 137 \\
&\equiv 104 \cdot 10 + 104 \cdot 3 \bmod 137 \\
&\equiv 1040 + 312 \bmod 137 \\
&\equiv -56 + 38 \bmod 137 \\
&\equiv -18 \bmod 137 \\
&\equiv 119 \bmod 137
\end{aligned}$$

$$\begin{aligned}
8 \cdot 13^3 \equiv 119 \cdot 13 \bmod 137 &\equiv -18 \cdot 13 \bmod 137 \\
&\equiv -18 \cdot 10 + (-18) \cdot 3 \bmod 137 \\
&\equiv -180 - 54 \bmod 137 \\
&\equiv -43 - 54 \bmod 137 \equiv -97 \bmod 137 \\
&\equiv \boxed{40 \bmod 137}
\end{aligned}$$

$8 \cdot 13^4 \equiv 40 \cdot 13 \bmod 137$

$\equiv 40 \cdot 10 + 40 \cdot 3 \bmod 137$

$\equiv 400 + 120 \bmod 137$

$\equiv -11 + (-17) \bmod 137$

$\equiv -28 \bmod 137$

$\equiv 109 \bmod 137$

$8 \cdot 13^5 \equiv 109 \cdot 13 \bmod 137$

$\equiv (-28)(13) \bmod 137$

$\equiv (-28)(10) + (-28)(3) \bmod 137$

$\equiv (-280) + (-84) \bmod 137$

$\equiv -6 + (-84) \bmod 137$

$\equiv -90 \bmod 137$

$\equiv 47 \bmod 137$

$\Longrightarrow \boxed{8, 104, 119, 40, 109, 47}$

5

Ideas in Mathematics
Math 170, Spring 2016
Assignment 10, part 1

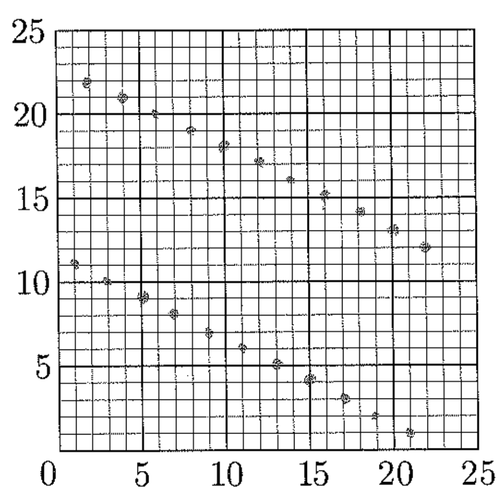
1. **Linear congruence generators** (LCG) generate pseudo-random numbers using modular arithmetic. For a fixed multiplier a, modulus m, and initial "seed" s, each "random" number is generated from the previous one using the recursive relation $x_{n+1} = ax_n \pmod{m}$; the first number is the seed, $x_0 = s$.

   For the given a, m, and s, compute x_0, x_1, x_2, x_3, x_4, and x_5.

   - $a = 3$, $m = 7$, $s = 4$ 4, 5, 1, 3, 2, 6
   - $a = 2$, $m = 13$, $s = 5$
   - $a = 10$, $m = 17$, $s = 4$
   - $a = 10$, $m = 15$, $s = 7$
   - $a = 11$, $m = 23$, $s = 3$
   - $a = 13$, $m = 137$, $s = 8$

2. **Spectral test.** Consider an LCG with $a = 11$ and $m = 23$. Choose any seed $0 < s < m$ and calculate all x_i. Then, on the graph below, plot all pairs of points (x_0, x_1), (x_1, x_2), $\ldots (x_{m-1}, x_0)$.

ANSWER IS INDEPENDENT OF CHOICE OF SEED



4. NEED TO FIGURE OUT $365 \bmod 7$

$$365 \equiv 365 - 350 \bmod 7 \equiv 15 \bmod 7$$
$$\equiv 1 \bmod 7$$

SO EACH YEAR, THE DAY SHIFTS BY

1

$\Longrightarrow$ APRIL 18 2017 IS TUESDAY

" " 2020 IS FRIDAY

" " 2050 IS SUNDAY

SINCE $30 \equiv 2 \bmod 7$

" " 2100 IS MONDAY

SINCE $50 \equiv 1 \bmod 7$

" " 3000 IS FRIDAY

SINCE $900 \equiv 200 \bmod 7 \equiv 60 \bmod 7$
$\equiv 4 \bmod 7$

5: THERE ARE MANY WAYS TO DO THIS. THE EASIEST IS PROBABLY DIVIDING THE OUTPUT OF THE LCG BY m.