Number Theory Inman Tutoring

1. $x_0 = 3$ $a = 1$, $c = 7$ $m = 12$

$x_{n+1} = (a x_n + c) \bmod m$

[illegible]

$x_1 = 3 \bmod 12 \cdot 1 \bmod 12 + 7 \bmod 12$

$= 1 \cdot 7 + 7$

$\boxed{x_1 = 8 \bmod 12}$

$x_2 = 1 \cdot 8 \bmod 12 + 7$

$= 8 + 7$

$\boxed{x_2 = 3} \bmod 12$

$x_3 = 1 \cdot 4 \bmod 12 + 7$

$\boxed{x_3 = 4}$

$x_4 = 1 \cdot 4 \bmod 12 + 7$

$4 + 7$

$\boxed{x_4 = 11}$

$x_5 = 1 \cdot 11 \bmod 12 + 7$

$11 + 7$

$\boxed{x_5 = 6}$

x_1, x_2, x_3, x_4, x_5
2, 3, 4, 11, 6

2. $100! = 100 \cdot 99 \cdot 98 \cdots$

we look 50 2's in 100

$100 = 50 \cdot 2$ ✓

How many terms in 100! divisible by 5?

$100 = 20 \cdot 5$ 20 terms divisible by 5

What about 25 or 5^2

$100 = 25 \cdot 4$

20 terms divisible by 5 5, 10, 15 ... 100

4 terms have an extra 5 (25, 50, 75, 100)

$20 + 4 = 24$

24 5's + 24 2's = 24 10's

so, there are 24 0's at the end of 100!

[illegible] $4n \cdot n^4 - 1$ [illegible] divisible by 5 [illegible]
$(5 \mid n^4 \dots)$

Case 1: $n \equiv 0 \bmod 5$
[illegible] $\equiv 0 \bmod 5$, [illegible]

Case 2: $n \equiv 1 \bmod 5$

$n^4 \equiv 1 \bmod 5$ $\quad -5n^4 \equiv 0 \bmod 5$ $\quad 4n \equiv 4 \bmod 5$
$1 + 4 \equiv 0 \bmod 5$

Case 3: $n \equiv 2 \bmod 5$ $\quad n^4 \equiv$ [illegible] $\bmod 5$ $\quad 4n \equiv 3 \bmod 5$
$2 + 3 \equiv 0 \bmod 5$

Case 4: $n \equiv 3 \bmod 5$ $\quad n^4 \equiv n(n^2)^2 \equiv 1 \bmod 5$ $\quad 4n \equiv 2 \bmod 5$
$3 + 2 \equiv 0 \bmod 5$

Case 5: $n \equiv 4 \bmod 5$ $\quad 4n \equiv 1 \bmod 5$ $\quad n^4 \bmod 5$ $\quad 1 + 4 \equiv 0 \bmod 5$

4. [illegible] $\bmod 11$ [illegible] [illegible] $\bmod 11 = 2$

$2^{[illegible]} \bmod 11$

$(2^{[illegible]})^{[illegible]} \bmod 11$

$(2 \cdot [illegible])^{2} \bmod 11$

$\left(2 \cdot (2^{[illegible]})\right)^{2} \bmod 11$

$\left(2 \cdot [(2^{[illegible]})^{2}]^{2}\right)^{2} \bmod 11$

$\left(2 \cdot [2 \cdot 2^{[illegible]}]\right)^{2} \bmod 11$

$\left(2 \cdot [(2 \cdot (2^{[illegible]})^{2})^{2}]\right)^{2} \bmod 11$

$(2\cdot[(1\cdot 2(3)^2)^2 \ldots]^2)^2 \bmod 11 =$

$(2\cdot[(1\cdot(4)^2)^2]^{[illegible]})^2 \bmod 11 =$

$(2\cdot[(10)^2]^2)^2 \bmod 11 =$

$(2\cdot[1]^2)^2 \bmod 11 =$

$(2^2) \bmod 11 =$

$4 \pmod{11}$

$\boxed{1385^{[illegible]} \equiv 4 \bmod 11}$

5. gcd(309, 112)

$309 = 112\cdot 2 + 85$

$112 = 85\cdot 1 + 27$

$85 = 27\cdot 3 + 4$

$27 = 4\cdot 6 + 3$

$4 = 3\cdot 1 + 1$

gcd(309, 112) = 1

$\downarrow$

$\boxed{\text{relatively prime}}$

6. $54x + 16y = \gcd(54, 16)$

$\gcd(54, 16)$:

$54 = 16 * 3 + 6$

$16 = 6 * 2 + 4$

$6 = 4 + 2$

$4 = 2 * 2 + 0$

$r_0 = 54$

$r_1 = 16$

$54 - 16 * 3 = 6$

$r_0 - 3r_1 = 6$

$r_1 - 6 * 2 = 4$

$6 - 4 = 2$

$r_1 - (r_0 - 3r_1) * 2 = 4$

$r_0 - 3r_1 - r_1 + (r_0 - 3r_1) * 2 = 2$

$3r_0 - 10r_1 = 2$

$x = 3$

$y = -10$

$54(3) + 16(-10) = 2$

7. $x = 33 \bmod 112$

$112 = 33 \times 3 + 13$

$33 = 13 \cdot 2 + 7$

$13 = 7 \cdot 1 + 6$

$7 = 6 + 1$

$6 = 1 \cdot 6 + 0$

$7 = 7r_1 - 2r_0$

$6 = r_0 - 3r_1 - 7r_1 + 2r_0$

$6 = 3r_0 - 10r_1$

$r_0 = 112$

$r_1 = 33$

$13 = r_0 - 3r_1$

$7 = r_1 - 2 \cdot 13$

$7 = r_1 - 2(r_0 - 3r_1)$

$6 = r_0 - 3r_1 - (r_1 - 2(r_0 - 3r_1))$

$1 = r_1 - 2(r_0 - 3r_1) - (r_0 - 3r_1 - (r_1 - 2(r_0 - 3r_1)))$

$7r_1 - 2r_0 - 3r_0 + 10r_1 = 17r_1 - 5r_0$

$-5r_0 + 17r_1 \bmod 112$

$x = -5$

$y = 17$

17 is multiplicative inverse of 33 mod 112