Problem 1: Number Theory

① $X_{n+1} = (a * X_n + c) \bmod m$

$a = 13$, $c = 7$, $X_0 = 5$, $m = 12$

$X_1 = (13 \cdot 5 + 7) \bmod 12 = \boxed{2}$

$X_2 = (13 \cdot 2 + 7) \bmod 12 = \boxed{9}$

$X_3 = (13 \cdot 9 + 7) \bmod 12 = \boxed{4}$

$X_4 = (13 \cdot 4 + 7) \bmod 12 = \boxed{11}$

$X_5 = (11 \cdot 13 + 7) \bmod 12 = \boxed{6}$

② Zeros are at the end of 100!

$100! \quad \frac{100}{5} = 20$ terms divisible by 5^1

$\frac{100}{25} = 4$ divisible by 5^2

$20 + 4 = 24$ factors 5 in 100!

100! div by 10^{24} no greater power of 10

100! ends with 24 zeros

③ $n^5 - 5n^3 + 4n$

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

$n(n^2-4)(n^2-1)$

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

Consecutive 5 numbers

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

must be div by 5

④ $1333^{42} \bmod 11$

$r_0 = 1333 \not\equiv 11$

$1333^2 \not\equiv 11$

$((1333)^{21})^2 \bmod 11$

$((1333)(1333)^{20})^2 \bmod 11$

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

$((1333)(1333(1333^5)^2)^2)^2 \bmod 11$

$((1333)(1333(1333(1333^4))^2)^2)^2$

$((2)^{21})^2 \bmod 11$

$(2(2^{10})^2)^2 \bmod 11$

$(2(2^5)^4)^2 \bmod 11$

$(2(32)^4)^2 \bmod 11$

$(2(00)^4)^2 \bmod 11$

$(2(100)^2)^2 \bmod 11$

$(2(1)^2)^2 \bmod 11$

$4 \bmod 11$

$\boxed{4}$

⑤ gcd Euclids

309 112
a b

r = 309 % 112 = 85
a = 112
b = 85
r = 112 % 85 = 27
a = 85
b = 27
r = 85 % 27 = 4
a = 27
b = 4
r = 27 % 4 = 1
a = 4
b = 1
r = 4 % 1 = 0
a = 1
b = 0
relatively prime

⑥ $54x + 16y = \gcd(54, 16)$

$54 = 3 \cdot 16 + 6$
$16 = 2 \cdot 6 + 4$
$6 = 1 \cdot 4 + 2$
$4 = 2 \cdot 2 + 0$
2

$r_0 = 54 \quad r_1 = 16$

$6 = 54 - 3 \cdot 16 = 1 \cdot r_0 - 3r_1$
$4 = 16 - 2 \cdot 6 = r_1 - 2(1 \cdot r_0 - 3r_1)$
$= r_1 - 2r_0 + 6r_1$
$= 7r_1 - 2r_0$
$2 = \gcd(54, 16) = 7r_1 - 2r_0$
$= 7(16) - 2(54)$

$x = -4 \quad y = 7$

$54 = 3 \cdot 16 + 6 \quad r_0 = 54$
$16 = 2 \cdot 6 + 4 \quad r_1 = 16$
$6 = 1 \cdot 4 + 2$
$4 = 2 \cdot 2 + 0$
2

$6 = 54 - 3 \cdot 16 = 1r_0 - 3r_1$
$4 = 16 - 2 \cdot 6 = r_1 - 2(1 \cdot r_0 - 3r_1)$
$= r_1 - 2r_0 + 6r_1$
$= 7r_1 - 2r_0$
$2 = 6 - 1 \cdot 4 = r_0 - 3r_1 - (7r_1 - 2r_0)$
$= r_0 - 3r_1 - 7r_1 + 2r_0$
$= 3r_0 - 10r_1$

$x = 3 \quad y = -10$

(7) Multiplicative Inverse of $x = 33 \bmod 112$

Multiplicative Inverse

33 mod 112

$x = 33 \quad m = 112$

$\gcd(33, 112) = 1$

$z \cdot m + y \cdot x = 1 \pmod m$

$z \cdot 112 + y \cdot 33 = 1 \pmod{112}$

$112 = 3(33) + 13 \Rightarrow 13 = 112 - 3(33) = r_1 - 3r_0$

$33 = 2(13) + 7 \Rightarrow 7 = 33 - 2(13) = r_0 - 2(r_1 - 3r_0) = r_0 - 2r_1 + 6r_0 = 7r_0 - 2r_1$

$13 = 1(7) + 6 \Rightarrow 6 = 13 - 1(7) = (r_1 - 3r_0) - (7r_0 - 2r_1)$

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

$= 3r_1 - 10r_0$

$7 = 1(6) + 1 \Rightarrow 1 = 7 - 1(6) = 7r_0 - 2r_1 - (3r_1 - 10r_0)$

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

$= 17r_0 - 5r_1$

$6 = 6(1) + 0$

$r_0 = 33 \;\; r_1 = 112$

Choose 17, as it is y value

Multiplicative Inverse = 17