0. Basis: $1! = 1$ \  \ 1 = 1 \ \ \ \ \sqrt{3}$

Inductive Step: Assume $n! \leq n^n - 3$

Want to prove $(n+1)! \leq (n+1)^{n+1}$

$(n+1)! = (n+1)n! \leq (n+1)n^n \leq (n+1)(n+1)^n = (n+1)^{n+1}$

By induction

1. $23 = 16 + 4 + 2 + 1$

Mod 7:

$5^2 = 25 = 4$
$5^4 = 4^2 = 16 = 2$
$5^8 = 2^2 = 4$
$5^{16} = 2$

$5^{23} = 5^{(6+4+2+1)} = 5^{16} \cdot 5^4 \cdot 5^2 \cdot 5 = \frac{2 \cdot 2 \cdot 4 \cdot 5}{4} = 10 = 3$

2. Euclid on 20 & 23:

$23 = 20 + 3$
$20 = 6 \cdot 3 + 2$
$3 = 2 + 1 \checkmark$

$1 = 3 = (20 - 6 \cdot 3) = 7 \cdot 3 - 20$

$= 7(23 - 20) - 20 = 7 \cdot 23 - 8 \cdot 20 \checkmark$

$\therefore 20^{-1} = -8 \mod 23$

$\therefore x \equiv -8 \cdot 5 = -40 = 6 \mod 23 \checkmark$
\[ x \equiv 3 \mod 4 \quad \implies \quad x \equiv 4 \mod 5 \quad \implies \quad x \equiv 5 \mod 6 \]

\[ x \equiv 5 \mod 2 \quad \land \quad x \equiv 2 \mod 3 \]

\[ x \equiv 3 \mod 4 \quad \quad k_1 = 15 \quad \quad m = 60 \]
\[ x \equiv 4 \mod 5 \quad \quad k_2 = 12 \]
\[ x \equiv 2 \mod 3 \quad \quad k_3 = 20 \]

**Euclid for 4 & 15:**
\[ 15 = 3 \cdot 4 + 3 \]
\[ 4 = 3 + 1 \]
\[ 3 = 15 - 3 \cdot 4 \]
\[ 1 = 4 - 3 = 4 - (15 - 3 \cdot 4) \]
\[ = 4 \cdot 4 - 15 \]
\[ \therefore k_1^{-1} = -1 \mod 4 \]
\[ \therefore x_1 = -1 \]

**Euclid for 5 & 12:**
\[ 12 = 2 \cdot 5 + 2 \]
\[ 5 = 2 \cdot 2 + 1 \]
\[ 2 = 12 - 2 \cdot 5 \]
\[ 1 = 5 - 2 \cdot 2 = 5 - 2(12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12 \]
\[ \therefore k_2^{-1} = -2 \quad \therefore x_2 = -24 \]

**Euclid for 3 & 20:**
\[ 20 = 6 \cdot 3 + 2 \]
\[ 3 = 2 + 1 \]
\[ 2 = 20 - 6 \cdot 3 \]
\[ 1 = 3 - 2 = 3 - (20 - 6 \cdot 3) = 7 \cdot 3 - 20 \]
\[ \therefore k_3^{-1} = -1 \quad \therefore x_3 = -20 \]

By the Chinese Remainder Theorem, the unique solution is
\[ x = 3(-15) + 4(-24) + 2(-20) = -181 = 59 \mod 60 \]

Alternate technique
\[ x \equiv -1 \mod 4 \]
\[ x \equiv -1 \mod 5 \]
\[ x \equiv -1 \mod 3 \]

\[ \therefore \text{By CRT} \quad x \equiv -1 \mod 60 \]

\[ \therefore \]
\[ x^5 + 1 = x^2(x^3 + 1) - x^2 + 1 \]

\[ \frac{x^5 + x^2}{-x^2 + 1} \]

\[ \frac{-x}{x^2 + 1} \]

\[ \frac{x^3 + 1}{(-1)(-x^2 + 1) + x + 1} \]

\[ x + 1 = x^3 + 1 - (-x)(-x^2 + 1) \]

\[ \text{gcd}(x^5 + 1, x^3 + 1) = x + 1 \]

\[ \text{Bezout:} \]

\[ x + 1 = x^3 + 1 + x(x^5 + 1 - x^2(x^3 + 1)) \]

\[ = (1-x^3)(x^3 + 1) + x(x^5 + 1) \]

\[ \text{It is enough to show that gcd}(a, b) \text{ and gcd}(a, r) \]

\[ \text{divide each other (assuming everything is positive)} \]

\[ \text{gcd}(a, b) | a \]

\[ \text{gcd}(a, b) | b \Rightarrow \text{gcd}(a, b) | b - aq = r \]

\[ \text{Conversely} \]

\[ \text{gcd}(a, r) | a \]

\[ \text{gcd}(a, r) | r \Rightarrow \text{gcd}(a, r) | aq + r = b \]
Suppose $a \neq 0$ and consider the sequence $a^n, n = 1, 2, \ldots$

By the pigeonhole principle, there exist $m, n < m$ with $a^n = a^m$.

Then $0 = a^m - a^n = a^n(a^{m-n} - 1)$

Suppose $a$ is not a zero divisor.

$\Rightarrow$ If $n = 1$, then $a^{m-n} - 1 = 0$, so $a^{m-n} = 1$ so $a$ is a unit.

$\Rightarrow$ If $n > 1$ write $0 = a a^{n-1}(a^{m-n} - 1)$

Then $0 = a^{n-1}(a^{m-n} - 1)$ so by reverse induction, $a$ is a unit.

$\therefore$ $a$ is a zero divisor or a unit.

To show that $a$ cannot be both.

Suppose $a$ is a unit and for some $b, a b = 0$.

Then $b = a^{-1} a b = a^{-1} 0 = 0$.

$\therefore$ $a$ is not a zero divisor.
8. \( U_4 = \{ 1, 3 \} \)

\[ 3^2 = 9 \equiv 1 \pmod{4} \] so \( U_4 \) is generated by 3.

\( (U_4 \cong \mathbb{Z}_2) \)

\[ S_3 = \{ (1), (1,2), (2,3), (1,3), (1,2,3), (1,3,2) \} \]

\[ (1,2)^2 = (1) \]
\[ (2,3)^2 = (1) \]
\[ (1,3)^2 = (1) \]
\[ (1,2,3)^2 = (1,3,2) \]
\[ (1,2,3)^3 = (1) \]
\[ (1,3,2)^2 = (1,2,3) \]
\[ (1,3,2)^3 = (1) \]

\( \therefore S_3 \) has no elements of order 6, so cannot be cyclic.

Alternate technique:

Since for any \( m, n \), \( a^m \cdot a^n = a^{m+n} = a^m \cdot a^n \) in cyclic groups are commutative, but \( S_3 \) is not, e.g.

\[ (1,2)(2,3) = (1,2,3) \]
\[ (2,3)(1,2) = (1,3,2) \]
$U_4 = \{1, 3\}$ acts on itself by multiplication.

1 $\mapsto (1)$
3 $\mapsto (1, 3)$

So define $f: U_4 \to S_3$ by

$f(1) = (1)$
$f(3) = (1, 3)$

\[f(1 \cdot 1) = f(1) = (1) = (1) \cdot (1) = f(1) \cdot f(1)\]
\[f(3 \cdot 3) = f(1) = (1) = (1,3)(1,3) = f(3) \cdot f(3)\]
\[f(1 \cdot 3) = f(3) = (1,3) = (1)(1,3) = f(1) \cdot f(3)\]

So $f$ is a hom.

Have a great Summer