

P6578708 (3)

$1 \in S$, for put $x=y=1$, then $1 \cdot 1 = 1$
 which makes $1 \in T$ impossible ✓
 (we would have $T \ni 1 \cdot 1 = 1 \in S$,
 clearly impossible for S, T disjoint) ✓
 Also from 1) the closure axiom
 to make S a group is satisfied. ✓
 Now if $x \in \mathbb{Z}_3$ (where \mathbb{Z}_3 is the
 set $\{1, \dots, 30\}$, then x has a
 unique multiplicative inverse $x^{-1} \pmod{3}$ since 3 is prime ✓
 $\Rightarrow x x^{-1} = 1 \pmod{3}$ is defined ✓
 Suppose $x \in S, x^{-1} \in T$, then
 from 3. we have $x x^{-1} = 1 \in T$ ✓
 but $1 \in S$, so we have a con-
 tradiction and $x^{-1} \in S$, so the
 inverse axiom is satisfied. ✓
 Modular multiplication is
 associative. S is a subgroup
 of \mathbb{Z}_3 , $X \cdot Y = A$ say.
 A is cyclic, with generator
 3, since $3^{143} \equiv -1 \pmod{31}$
 (for every divisor of 143)
 $\therefore A$ has a unique subgroup, also
 cyclic. In fact every subgroup of A is
 cyclic. The composition of each
 subgroup depends on the powers
 of the generator in it. Is $3 \in S$?
 No, for if it were then $3^2, 3^3, \dots$
 in fact every power of 3 would
 be in S and T would be empty ✓
 $\therefore 3 \in T$. from 2, $3^2 \in S$, from 3, $3 \cdot 3 \in T$
 etc, with every odd power of 3 a
 member of T , every even power
 a member of S .
 $\Rightarrow S = \{3^2, 3^4, 3^6, 3^8, 3^{10}, 3^{12}, 3^{14}, 3^{16}, 3^{18}, 3^{20}, 3^{22}, 3^{24}, 3^{26}, 3^{28}, 3^{30}\}$
 reduced mod 31 ✓

Not quite enough
 need to check
 $\phi(31)/p$
 for all
 $p \mid \phi(31)$
 $p = 2, 3, 5$