# FINAL MAT 3233 Sp. 2005

(1) Basis $1! = 1$ $1^1 = 1$ ✓ ✓ 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 ✓ 4

(2) $23 = 16 + 4 + 2 + 1$

Mod 7: $5^2 = 25 = 4$

$5^4 = 4^2 = 16 = 2$

$5^8 = 2^2 = 4$

$5^{16} = 2$

$5^{23} = 5^{16+4+2+1} = 5^{16} \cdot 5^4 \cdot 5^2 \cdot 5 = \underbrace{2 \cdot 2}_{4} \cdot 4 \cdot 5 = 10 = 3$ (with $16 = 2$)

(3) Euclid on 20 & 23: ✓ 2

$23 = 20 + 3$ $\quad 3 = 23 - 20$

$20 = 6 \cdot 3 + 2$ $\quad 2 = 20 - 6 \cdot 3$

$3 = 2 + 1$ ✓ 3 $\quad 1 = 3 - 2$

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

$= 7(23 - 20) - 20 = 7 \cdot 23 - 8 \cdot 20$ ✓ 3

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

$\therefore x \equiv -8 \cdot 5 = -40 = 6 \mod 23$ ✓ 2

(4) $x \equiv 3 \bmod 4$ — implies → $x \equiv 5 \bmod 2 \equiv 1 \bmod 2$ ← drop ✓

$x \equiv 4 \bmod 5$

$x \equiv 5 \bmod 6$ → $x \equiv 5 \bmod 3 \equiv 2 \bmod 3$ ✓

5

---

$x \equiv 3 \bmod 4$ $\quad k_1 = 15$

$x \equiv 4 \bmod 5$ $\quad k_2 = 12$ ✓ $\quad m = 60$

$x \equiv 2 \bmod 3$ $\quad k_3 = 20$

---

Euclid for 4 & 15:

$15 = 3 \cdot 4 + 3$ $\qquad 3 = 15 - 3 \cdot 4$

$4 = 3 + 1$ $\qquad 1 = 4 - 3 = 4 - (15 - 3 \cdot 4)$

$= 4 \cdot 4 - 15$

$\therefore k_1^{-1} = -1 \bmod 4$ ✓

$\therefore x_1 = -15$

---

Euclid for 5 & 12

$12 = 2 \cdot 5 + 2$ $\qquad 2 = 12 - 2 \cdot 5$

$5 = 2 \cdot 2 + 1$ $\qquad 1 = 5 - 2 \cdot 2 = 5 - 2(12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12$ ✓

$\therefore k_2^{-1} = -2, \quad x_2 = -24$

---

Euclid for 3 & 20

$20 = 6 \cdot 3 + 2$ $\qquad 2 = 20 - 6 \cdot 3$

$3 = 2 + 1$ $\qquad 1 = 3 - 2 = 3 - (20 - 6 \cdot 3) = 7 \cdot 3 - 20$ ✓

$\therefore k_3^{-1} = -1, \quad x_3 = -20$

---

By the Chinese Rmdr thm the unique solution is

$x = 3(-15) + 4(-24) + 2(-20) = -181 \equiv 59 \bmod 60$

✓2

Alternate technique the system is equiv. to

$x \equiv -1 \bmod 4$

$x \equiv -1 \bmod 5$ $\quad \therefore$ By CRT $x \equiv -1 \bmod 60$

$x \equiv -1 \bmod 3$

☺

(5)

$$x^3+1 \;\overline{)\; x^5+1 \;}\; x^2$$

$$\underline{x^5+x^2}$$

$$-x^2+1$$

✓

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

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

$$-x^2+1 \;\overline{)\; x^3+1 \;}\; -x$$

$$\underline{x^3-x}$$

$$x+1$$

✓

$\therefore x^3+1 = (-x)(-x^2+1)+x+1$

$\therefore x+1 = x^3+1-(-x)(-x^2+1)$

$$x+1 \;\overline{)\; -x^2+1 \;}\; -x+1$$

$$\underline{-x^2-x}$$

$$x+1$$

$$\underline{x+1}$$

$$0$$

✓

✓

$\therefore \gcd(x^5+1, x^3+1) = \underline{x+1}$

Bezout:

$x+1 = x^3+1+x(x^5+1-x^2(x^3+1))$ ✓

$= \underline{(1-x^3)(x^3+1)+x(x^5+1)}$

(6) It is enough to show that $\gcd(a,b)$ & $\gcd(a,r)$ divide each other (assuming everything is positive) ☺

$\gcd(a,b) \mid a$

$\gcd(a,b) \mid b \Rightarrow \gcd(a,b) \mid b-aq = r$

$\Big\} \gcd(a,b) \mid \gcd(a,r)$

Conversely

$\gcd(a,r) \mid a$

$\gcd(a,r) \mid r \Rightarrow \gcd(a,r) \mid aq+r = b$

$\Big\} \gcd(a,r) \mid \gcd(a,b)$

(7) Suppose $a \neq 0$ & consider the sequence $a^n$, $n = 1, 2 \ldots$ /6.

By the pigeonhole principle $\exists n, m$ $n < m$ $a^n = a^m$

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

---

Suppose $a$ is not a zero divisor.

→ If $n = 1$, then $a^{m-n} - 1 = 0$, so $a^{m-n} = 1$

So $a$ is a unit

→ 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.

∴ $a$ is a zero divisor or a unit

---

To show that $a$ cannot be both

Suppose $a$ is a unit and

for some $b$ $ab = 0$.

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

∴ $a$ is not a zero divisor.

(8) $U_4 = \{1, 3\}$ ✓

$3^2 = 9 = 1$ so $U_4$ is generated by 3.

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

$S_3 = \{ (), (1,2), (2,3), (1,3), (1,2,3), (1,3,2) \}$

$(1,2)^2 = ()$
$(2,3)^2 = ()$
$(1,3)^2 = ()$
$(1,2,3)^2 = (1,3,2)$
$(1,2,3)^3 = ()$
$(1,3,2)^2 = (1,2,3)$
$(1,3,2)^3 = ()$

$\therefore$ $S_3$ has no elements of order 6 so cannot be cyclic.

Alternate technique:

Since for any $m, n$ $a^n \cdot a^m = a^{n+m} = a^m \cdot a^n$ cyclic groups are commutative, but $S_3$ is not, e.g. $(1,2)(2,3) = (1,2,3)$ $(2,3)(1,2) = (1,3,2)$ #

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

$1 \mapsto ()$

$3 \mapsto (1,3)$

So define $f: U_4 \to S_3$ by

$f(1) = ()$

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

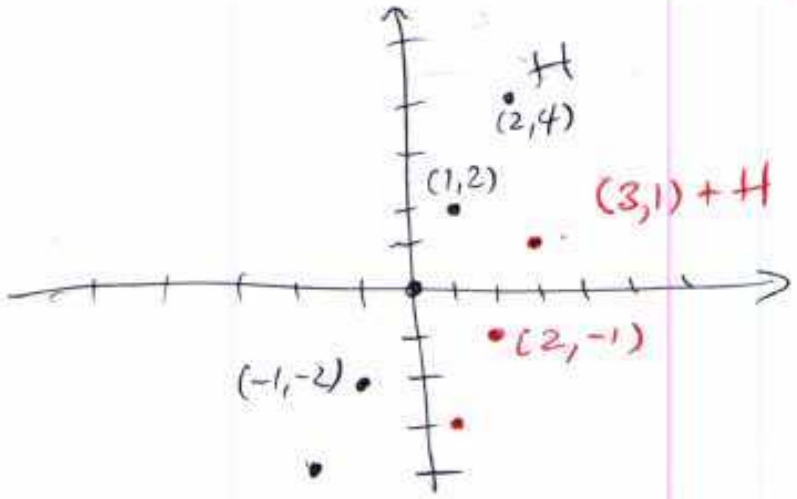
$f(1 \cdot 1) = f(1) = () = () \cdot () = f(1) \cdot f(1)$

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

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

So $f$ is a hom.

(10)




Have a great

Summer