Ej 19:

G grupo
$H < G$

a) qvq $H \triangleleft G$ si G abeliano

$H \triangleleft G \Rightarrow H < G$ ✓ $\wedge$ $aHa^{-1} \subseteq H \ \forall a \in G$
$aHa^{-1} \subseteq H \Rightarrow aha^{-1} \in H \ \forall a \in G$
G abeliano y $H < G \Rightarrow H$ abeliano $\Rightarrow aha^{-1} = aa^{-1}h = eh = h \in H$
$\therefore H \triangleleft G$

b) qvq $H \triangleleft G$ si $[G:H] = 2$
$\hookrightarrow o(G/H)$
$H \triangleleft G \Rightarrow H < G$ ✓ y $aH = Ha \ \forall a \in G$

$o(G/H) = 2$
$\hookrightarrow G/H = \{gH : g \in G\} = \{eH, gH\} = \{H, gH\}$ ($e \in G$)
$= \{Hg : g \in G\} = \{H, Hg\}$ (def. de G/H)

$\therefore gH = Hg$ para g cualquiera $\Rightarrow H \triangleleft G$

c) qvq
1. $\varphi: G \to G'$ morfismo
2. G' abeliano
3. $H < G$ tq $\ker(\varphi) \subseteq H$

$\Rightarrow H \triangleleft G \to H < G \wedge aHa^{-1} \subseteq H$ ∴ $aH = Ha \ \forall a \in G$

1. $\varphi: G \to G'$ morfismo $\Rightarrow \varphi(\overset{\text{op } G}{ab}) = \varphi(a)\overset{\text{op } G'}{\varphi(b)} \underset{2.}{=} \varphi(b)\varphi(a) \underset{1.}{=} \varphi(ba)$
2. $ab = ba \ \forall a, b \in G'$
3. $\ker(\varphi) = \{x \in G : \varphi(x) = e_{G'}\} \subseteq H$

$\{aha^{-1} : h \in H, \ a \in G\} \subseteq H$

qvq $aha^{-1} \in \{x \in G : \varphi(x) = e_{G'}\}$ $\approx$ $\varphi(aha^{-1}) = e_{G'}$

$$\varphi(aha^{-1}) \overset{\text{asoc.}}{=} \varphi((ah)a^{-1}) \overset{2.}{=} \varphi(a^{-1}(ah)) \overset{\text{asoc.}}{=} \varphi((a^{-1}a)h) = \varphi(e_G h) = \varphi(h)$$

$H < G \Rightarrow ab^{-1} \in H \ \forall a, b \in H$

Ej 22:

a) $S = \begin{cases} x \equiv 3 \ (10) \\ x \equiv 1 \ (11) \\ x \equiv 2 \ (7) \end{cases}$

1. 10, 11 y 7 son coprimos

2. $S_1 = \begin{cases} x \equiv 3 \ (10) \\ x \equiv 0 \ (11) \\ x \equiv 0 \ (7) \end{cases}$ $S_2 = \begin{cases} x \equiv 0 \ (10) \\ x \equiv 1 \ (11) \\ x \equiv 0 \ (7) \end{cases}$ $S_3 = \begin{cases} x \equiv 0 \ (10) \\ x \equiv 0 \ (11) \\ x \equiv 2 \ (7) \end{cases}$

3. resuelvo S_1

   a. $m' = 11 . 7 = 77$

   b. qvq $v' / m'v' \equiv 1 \ (10)$

   $77 v' \equiv 1 \ (10)$

Aplico Alg. Euclides para hallar $mcd(10, 77)$

$77 = 7 . 10 + 7$

$10 = 1 . 7 + 3$

$7 = 2 . 3 + 1$ //

$1 = 7 - 2.3$
$= 7 - 2.(10 - 1.7)$
$= 7 - 2.(10 - 7)$
$= 7 - 20 + 2.7$
$= 7.(1+2) - 2.10$
$= 3.(77 - 7.10) - 2.10$
$= 3.77 - 3.7.10 - 2.10$
$= \underline{77}.3 - \underline{10}.19$
$\therefore v' = 3$

c. $x_1 = a_1 . v' . m'$
$= 3.3.77$
$= 693$

4. resuelvo $S_2 = \begin{cases} x \equiv 0 (10) \\ x \equiv 1 (11) \\ x \equiv 0 (7) \end{cases}$

a. $m' = 7.10 = 70$
b. $v' / m'v' \equiv 1 (11)$
$70 v' \equiv 1 (11)$

Aplico euclides para mcd (11,70)
$70 = 6.11 + 4$
$11 = 2.4 + 3$
$4 = 1.3 + 1$ //

$$1 = 4 - 1.3$$
$$= 4 - 11 + 2.4$$
$$= (1+2).4 - 11$$
$$= 3.(70 - 6.11) - 11$$
$$= 3.70 - 3.6.11 - 11$$
$$= 70.3 - 11.(9-1)$$
$$= \underline{70}.3 - \underline{11}.8$$

$\therefore v' = 3$

c. $x_2 = a_2 . v' . m'$
$$= 1.3.70$$
$$= 210$$

5. resuelvo
$$S_3 = \begin{cases} x \equiv 0 \ (10) \\ x \equiv 0 \ (11) \\ x \equiv 2 \ (7) \end{cases}$$

$m' = 10.11 = 110$

$110 \, v' \equiv 1 (7)$

Euclides para mcd(110,7)

$$110 = 15.7 + 5$$
$$7 = 1.5 + 2$$
$$5 = 2.2 + 1 //$$

$$1 = 5 - 2.2$$
$$= 5 - 2.(7 - 5.1)$$
$$= 5 - 2.7 + 2.5.1$$
$$= 5.(1+2) - 2.7$$

$= 3.(110-15.7)-2.7$

$= 3.110 - 15.7.3 - 2.7$

$= 3.110 - 7.(15.3-2)$

$= 3.\underline{110} - \underline{7}.43$

$\therefore v' = 3$

$x_3 = a_3 . v' . m'$

$= 2.3.110$

$= 660$

$\therefore x_1 = 693$

$x_2 = 210 \qquad \Rightarrow x_0 = 1563$

$x_3 = 660$

$m = 10.11.7 = 770$

$\tilde{x} = 1563 + k.770 \qquad k = 1 \Rightarrow \tilde{x} = 2333$

$\tilde{x} \equiv 1563\ (770)$

$2333 = k.10 + 3 \Rightarrow k = 233$

$2333 = k'.11 + 1 \Rightarrow k' = 212$

$2333 = k''.7 + 2 \Rightarrow k'' = 333$

Teorema: Peq. T. de Fermat

sea p primo y $a \in \mathbb{Z} / p \nmid a \Rightarrow a^{p-1} \equiv 1\ (p)$

a no divisible por p

Corolario:

p primo y $a \in \mathbb{Z} \Rightarrow a^p \equiv a\ (p)$

$a^{kp} \cdot a^{-k} \cdot a^{r} = k'p + a^{r}$ 2.

$(k\,kp + a) \cdot (k \cdot -k + a) \cdot (k\,r + a) = k'p + a^{r}$

$(k\,kp \cdot (-k\,k) + k\,kp \cdot a + a(-k\,k) \cdot a^{2}) \cdot (k\,r + a)$

$a \equiv b(c)$

$a/c \to b$

Ej. 20. Sea p un número primo y $a \in \mathbb{Z}$ tal que $p \nmid a$. Probar que:

a) Si $n \equiv r\ (p-1)$, entonces $a^n \equiv a^r\ (p)$.

b) Concluir en particular que $a^n \equiv a^{r_{p-1}(n)}\ (p)$.

a) qpq $n \equiv r(p-1) \Rightarrow a^n \equiv a^r(p)$

$n - r = k \cdot (p-1)$ $\qquad$ $a^n - a^r = k' \cdot p$

$n = k \cdot (p-1) + r$ 3.

por corolario y teorema tenemos

$a^{p-1} \equiv 1\ (p)$ $\qquad$ $a^p \equiv a(p)$

$a^{p-1} - 1 = k \cdot p$ 1. $\qquad$ $a^p - a = kp$ 2.

$a^n \equiv a^r(p)$ 3.

$a^{k\cdot(p-1)+r} \equiv a^r(p)$

$a^{kp-k+r} = k'p + a^r$ $\qquad$ $a^{k(p-1)} = {a^{(p-1)}}^{k}$

$a^{k(p-1)+r} = k'p + a^r$ $\qquad$ $= (kp+1)^k$

$a^{k(p-1)} \cdot a^r - a^r = k'p$

$a^r \cdot (a^{k(p-1)} - 1) = k'p$ $\qquad$ $a^r \cdot (kp+1)^k$

$a^r \cdot ((kp+1)^k - 1) = k'p$