P3 Examen Sección 1/

$ab - 1 = x^3$

$ab = x^3 + 1$

En la sección hay redacción

$2^{2n} - 1$

$n = 2$ $\quad \sqrt[3]{2^{2n} - 1}$

1, 2, 3, 4

$3 \cdot 1 - 1 = 2$

$3 \cdot 2 - 1 = 5$

$b - 1$

$2b - 1$

$3b - 1$

$bk - 1 = (k(2^{n-1})) - 1$

$x < \sqrt[3]{k} \cdot \sqrt[3]{2^{n-1}}$

$2^{\frac{n-1}{3}}$

$kb - 1 - (\ell b - 1)$

$b(k - \ell)$ ← diferencia de cubos

x es al máximo $2^{\frac{3}{3}n}$

$= (a-b)(a^2 + ab + b^2)$

$(x-y)(x^2 + xy + y^2)$ ←

$x^3 - y^3$

P3 Enunciado Socio 21

$ab - 1 = x^3$

$ab = x^3 + 1 \equiv 0 \mod b$

$\Rightarrow x^3 \equiv -1 \mod b$

$(x+1)(x^2 - x + 1)$

$-x^2 - x$

$-2x + 1$

$2x + 2$

3

1 solución

$+1 \pm \sqrt{-3}$ ¿-3 es cuad mod b?

2

$x^2 - x + 1 \equiv y^2 - y + 1$

$x^2 - y^2 - x + y$

$(x-y)(x+y-1) = 0$

P3 Enunciado B. Serie 3)

$x^3 - y^3 \equiv 0 \mod b$

$(x-y)(x^2+xy+y^2)$

$-x^2+xy$

$2xy+y^2$

$-2xy-y^2$

$3xy$

Sean b_1, b_2 los divisores de b

Vemos $y \equiv -1$

¿Existe a tal que $a \equiv -1 \mod b_1$ y $a \not\equiv -1 \mod b_2$?

$(x+1)(x^2-x+1)$

Que pasa si -3 es cuad. de dos

No existe a con $a \equiv -1 \mod b_1$, $a \not\equiv -1 \mod b_2$

$3 \mid x+1$ $\quad y^2 - y + 1 \equiv 0 \mod 3$

$\Rightarrow$ 2 sols $\mod b$

n° 3 Examen oral Sujet n°1

Si $a^3 \equiv -1 \mod b_1$

$a^3 \equiv -1 \mod b_2$

$\Rightarrow a^3 \equiv -1 \mod b_1 b_2$ $\quad > 2^{2n-2}$

$(a-1)(a^2+a+1) \equiv 0 \mod b_1 b_2$

$2^{2n} - 2^n + 1$

~~$b_1 b_2$~~

Soit $d = \gcd(b_1, b_2)$

$c_1 = \frac{b_1}{d}$ $\quad c_2 = \frac{b_2}{d}$

$2^{2n-2} = 3 \cdot 2^{n-1}$

$2^n / 2^{n-1}$

7

$a^3 \equiv -1 \mod c_1$

$a^3 \equiv -1 \mod c_2$

$a^3 \equiv -1 \mod \frac{b_1 b_2}{d}$ $\quad \text{ppcm}(b_1, b_2)$

$c_1 b_2$

P3 - Socio 5) Ejercicio

$(a-1)$ (a^4+a+1)

1 $c_1 b_2$

c_1 b_2

b_2 c_1

$c_1 b_2$ 1

$a-1$ a^2+a+1

$-a^2+a$

1

$x^3 \equiv 1 \mod p$

$x^6 \equiv 1 \mod p$

order

$x^2 \equiv 1$

$x^3 \equiv x \equiv -1$

2 ó 6

$6 \mid p-1$

$p \equiv 1 \mod 6$

$\varphi(6) = 2$

$p = 7$

1 1

2 4 1

3 2 -1

y si comprobar 3 ?

mcd 8

1 1

2 0

3 3

0

-3

2

-1

mcd 9

1

-1

0

Si

3

$a \mid c_1 b_2$

$a \mid b_2$

$\frac{c_1}{3} \cdot b_2$

P4 Enunciado B. Sacco 61

$a_1, a_2, \dots a_{n+1}$ los elementos de A

$2^{n-1} - 1 < a_1 b_1 - 1 = x^3 < 2^{2n} - 1$

$\sqrt[3]{2^{n-1}-1} < x < \sqrt{2^{2n}-1}$

$x^3 \equiv -1 \mod b_1, b_2$

$a_1 b_2 - 1 = y^3$

$a_1 b_1 - 1 = x^3$

$a_1(b_2 - b_1) = (y-x)(y^2 + xy + x^2)$

$a_1^2 b_2 b_1 - a_1(b_1 + b_2) + 1$ → absurdo

$x^2 + x + 1 \equiv y^2 + y \pmod{}$

$(x-y)(x+y+1) \equiv 0$

$b_1 - 1 \leq x^3 \leq 2^n b_1 - 1 < 2^n b_1$

$x < 2^{\frac{n}{3}} \sqrt[3]{b_1} < 2^{\frac{2n}{3}} < 2^{n-1}$

$< b_1$

$\frac{2n}{3} < n - 1$

$1 < \frac{n}{3}$ $3 < n$ ✓

p4 Emmenel 3. Sucio 7

b, | ~~$(x-1)(x^2+x+1)$~~

$(x+1)(x^2-x+1)$

$\gcd(x-1, x^2-x+1) \mid 3$

mod 6

si gcd es 1

1	1
2	2
3	3
4	4
-1	-1

~~mod 19~~

b, |

1	1
2	8
3	8
4	7
5	11
6	7
7	

$(x-1)(x^2+x$

8 → 19

$19 \overline{)634}$ 3, 7

$19 \overline{)56}$ 2, 8

$(x+1)(x^2-x+1)$ mod p^k

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

$-x^2-x$

$-2x+1$

$+2x+2$

3

si $p \neq 3$

$p^k \mid \Rightarrow x \equiv -1$ mod p^k

$1 \quad p^k$

$\frac{1 \pm \sqrt{-3}}{2}$ mod p^k $(x+1)(x-2)+3$

P3 Emmanuel Sucio 91

$a(b+2^{n-1}) - 1$

$= ab + a2^{n-1} - 1$ ← cubo ?

$a_i b_i - 1 = x_i^3$ $\quad b_i = \frac{x_i^3+1}{a_i}$

$a_i = \frac{x_i^3+1}{b_1} = \frac{y_i^3+1}{b_2}$

$\frac{x_i^3+1}{y_i^3+1} = \frac{b_1}{b_2}$

$(a+2^{n-1})^3$

$= a^3 + 2^n a 2^{2n-2} + 3 \cdot 2^{n-1} a^2$

$2^0 = 1$

① ①

$2^1 = 2$

0 0
1 1

$2^2 = 4$

0 0
1 1
2 0
-1 -1
0 0

$2^3 = 8$

0 0
1 1
2 0
3 3
4 0
5 5
6 0
-1 -1
6

P3 Emmanuel Sucro a)

$a_1 b_1 - 1 = x_1^3$

$a_2 b_1 - 1 = x_2^3$

$\vdots$

$b_1(a_1 + a_2 + \dots + a_{n+1}) - (n+1) = x_1^3 + x_2^3 + \dots + x_{n+1}^3 > 2^{n-1}$ (S)

$b_2(a_1 + a_2 + \dots + a_{n+1}) - (n+1) = y_1^3 + y_2^3 + \dots + y_{n+1}^3$

$b_1 > b_2$

$(a_1 + a_2 + \dots + a_{n+1})(b_1 - b_2) = x_1^3 - y_1^3 + x_2^3 - y_2^3 + \dots > 2^{n-1}$ (S)

$< 2^{2n-1} - n$

$x_1^3 = b_1 a_1 - 1 \geq 2^{n-1} \cdot a_1$

$(x_1 + 1)^3 = x_1^3 + 3x_1^2 + 3x_1 + 1$

$3x_1^2 + 3x_1 + 1$

$3 \cdot 2^{\frac{n-1}{3} \cdot 2} + 3 \cdot 2^{\frac{n-1}{3}} + 1$

$x_1^3 - y_1^3 = a_1(b_1 - b_2)$

P3 Examen Sacio 101

$b_1 = 2^{n-1} + c_1$

$2^{a-1} \cdot a_1 + c_1 a_1 - 1$

2^{2n} $\qquad$ $2^{n/3}$

$x_1^3 \leq 2^n b_1 - 1 < 2^n b_1$

$x_1 \leq \sqrt[3]{b_1 \cdot 2^n} < 2^{2n/3}$

$1^3, 2^3, 3^3, \ldots, 2\lfloor \sqrt[3]{2^n \cdot b_1} \rfloor^3$ ← Cuentos son multiplos de b_1 y de b_2

$\lfloor \sqrt[3]{2^n \cdot b_1} \rfloor^3$

$1^3, 2^3, \ldots$ $\qquad$ $3 \cdot \lfloor \frac{2^n}{3} \rfloor$ $\qquad$ 2

P3 Funcional

Serie III

a) $\frac{x^3-1}{b_1} = \frac{y^3-1}{b_2}$

$x^3 - 1 = a_1 b_1$

$y^3 - 1 = a_1 b_2$

$x^3 - y^3 = a(b_1 - b_2)$

$x^3 + y^{3-2} = a_1(b_1 + b_2) > 2^n a_1$

$b_1 a_1 \quad b_1 a_2 \quad b_1 a_3 \cdots b_1 a_{n+1}$

son distintos cubos

$b_1 a_2 > (x+1)^3 \cdot x^3 : 3x^2 + 3x + 1 > 3x^2 \Rightarrow 3 b_1^{2/3} a_1^{2/3}$

$a_2 > \frac{3 a_1^{2/3}}{\sqrt[3]{b_1}}$

$x \geq \sqrt[3]{b_1 a_1}$

$2^n a_n > \frac{3^{y-1} a_1^{2/3}}{\sqrt[3]{b_1^{y-1}}}$

$a_3 > \frac{3 a_2}{\sqrt[3]{b_1}} \Rightarrow \frac{3 \cdot \left(\frac{3 a_1^{2/3}}{\sqrt[3]{b_1}}\right)}{\sqrt[3]{b_1}} = \frac{9 a_1^{2/3}}{\sqrt[3]{b_1^2}}$

P3 Ismael Socio 121

$$2^n \geq \frac{3^n a_1^{2/3}}{\sqrt[3]{b_1^n}}$$

$$\left(\frac{2\sqrt[3]{b_1}}{3}\right)^n > a_1^{2/3}$$

$$b_2 a_2 \geq b_1 a_1 + 3x^2 > b_1 a_1 + 3\sqrt[3]{b_1^2 a_1^2}$$

$$a_2 > a_1 + \frac{3\sqrt[3]{a_1^2}}{\sqrt[3]{b_1}}$$

$$x^3 b_2 - b_2 = y^3 b_1 - b_1$$

$$x^3 b_2 - y^3 b_1 - b_2 + b_1 = 0$$

$$(x^3 - y^3) b_2 + y^3 b_2 - y^3 b_1 - b_2 + y_1 = 0$$

$$(x^3 - y^3) b_2 + (b_2 - b_1)(y^3 - 1) = 0$$

$$(x^3 - y^3) b_2 = (y^3 - 1)(b_1 - b_2)$$

~~x>y~~

$x > y$

$b_1 > b_2$

P3 Emerald Sucio (3)

$(y^3-1)(a_1-b_2) < b_2(y^3-1)$

$(x^3-y^3) < y^3-1$

$x^3 < x^3+1 < 2y^3$

$\left(\frac{x}{y}\right)^3 < 2$

$\frac{x}{y} < \sqrt[3]{2}$

Pero $x > 2^{n/3}+1$

$y > 2^{n/3}$

$y^3 < x^3 < 2y^3$

$y^{3a} = ab_2 - 1$

$= ab_2 - 3$

$ab_1 - ab_2$

$\frac{y^3-1}{x^3-y^3} \geq \frac{ab_2-3}{a(b_1-b_2)} = \frac{b_2}{b_1-b_2}$

$ab_2 - 3 \geq ab_1$

P3 Entrenet Sucio (4)

$$ab_1 - 1 = x^3 b_1$$

$$ab_2 - 1 = y^3 b_2$$

$$a = \frac{x^3+1}{b_1} = \frac{y^3+1}{b_2}$$

$$x^3 b_2 + b_2 = y^3 b_1 + b_1$$

$$x^3 b_2 - y^3 b_1 + b_2 - b_1 = 0$$

$$(x^3 - y^3)(b_2) + (b_2 - b_1)(y^3+1) = 0$$

$x > y$, $b_1 > b_2$

$$(x^3 - y^3)(b_2) = (y^3+1)(b_1 - b_2) < b_2(y^3+1)$$

$$\frac{b_2}{b_1 - b_2} = \frac{y^3+1}{x^3 - y^3}$$

$$x^3 < 2y^3 + 1$$

$$x^3 - 1 > 2y^3$$

x, y están entre $2^{n/3}$ $2^{2n/3}$

P3 Examen Serie 15

$$(x^3 y^3)\, b_2 > 2^n (b_1 + b_2)$$

$$\frac{x^3 - y^3}{y^3 + 1} = \frac{b_1 - b_2}{b_2} = \frac{b_1}{b_2} - 1$$

$$\frac{x^3 + 1}{y^3 + 1} = \frac{b_1}{b_2}$$

$$x^3 \equiv -1 \mod b_1$$

$$2^{n/3} \leq x \leq 2^{2n/3}$$

y ≥ 2

Si $a \geq b$

Si $x < b$

$x > y$

$a b + 1 = x^3 < b^3$

$ab > ab + 1 = x^3 > b^3 > 2^{3(n-1)}$

$a > b^2$

P3 Enunciado B. Sucio 1/

Entonces $x < b$

$$b_1 = \frac{x^3+1}{9} > \frac{x^3}{9} \qquad \frac{b^{3x}}{4} > \frac{2^{\frac{3(n-1)}{2}}}{9}$$

$x^2 - x + 1$

Cx

$2x$

$4x^2 - 4x + 4$

$((2x-1)^2 + 3)(x-1) \equiv 0 \mod b_1$

$ab_1 - 1 \qquad ab_2 - 1$

$a_1 b_1 - 1 = a_2 b_2 - 1$

$a_2 b_1 - 1$

$2 \overset{?}{\Rightarrow} m$

Alo mas

$\log_2(n)$

3 n^2 $\log_2(n)$ 4

P 3 Em a red B. Sean (7/

Cuando -3 es res cuad.

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\cdot\frac{(3-1)}{2}} = (-1)^{\frac{(p-1)}{2}}$$

Si $p \equiv 1 \mod 4$

$$\left(\frac{-1}{p}\right) = 1$$

$$(-1)^{\frac{p-1}{2}} = 1$$

$$\Rightarrow \left(\frac{-3}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \mod 3 \\ -1 & \text{si } p \equiv -1 \mod 3 \end{cases}$$

Si $p \equiv -1 \mod 4$

$$\left(\frac{-1}{p}\right) = -1$$

$$(-1)^{\frac{p-1}{2}} = -1$$

$$\Rightarrow \left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right) = -\left(-\left(\frac{p}{3}\right)\right) = \left(\frac{p}{3}\right)$$

P3 Financial 3. seçim (8)

x^3

$ab_1 - 1$ $ab_2 - 1$ $\quad b_1 < b_2$

$a_1 < a_2 \dots < a_{n+1}$

$a_{n+1}b_2 - 1$ y^3

$a_{n+1}b_2 - a_1b_1 = y^3 - x^3$

$y > (x+(n+2))$

$y^3 - x^3 > +3x^2(n+2) + 3x(n+2)^2 + 1$

$y \; x > 2^{n/3}$

$(2^{n-1}+a)(2^{n-1}+b) - 1$

$2^{2n-2} + 2^{n-1}b - 2^{n-1}a - ab - 1$

P3 Emanuel Socio 19/

⊙ $ab-1 = x^3$

Lo vemos modulo b

$ab \equiv x^3+1 \mod b$

Entonces queremos contar soluciones

hay de eso

si $p \mid b$

$p \mid (x-1)(x^2+x+1)$

$\Rightarrow x \equiv 1 \mod p$

ó $x^2+x+1 \equiv 0 \mod p$

$\Rightarrow (2x+1)^2+3 \equiv 0 \mod p$

Entonces -3 es residuo cuad $2 = par$

mcd p pero

mcd segunda

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{+3}{p}\right) = \left((-1)^{\frac{p-1}{2}}\right)\left(\frac{(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}}{\left(\frac{p}{3}\right)}\right) = \frac{(-1)^{\left(\frac{p-1}{2}\right)\left(1+\frac{2}{2}\right)}}{\left(\frac{p}{3}\right)}$$

$$= \frac{1}{\left(\frac{p}{3}\right)} = \left(\frac{p}{3}\right)$$

P3 Encuentra B sea 20/

Entonces para ~~[illegible]~~ $p \mid b$

o $x \equiv 1 \mod p$

ó $x^2+x+1 \equiv 0 \mod p$

si ~~[illegible]~~ p es res. cuad mod 3.

Tiene 2 soluciones

Tiene 1 solucion

Entonces hay al menos 2 primos 1 mod 3 que dividen a b

:(

~~Si [illegible]~~

sin el -1 porque $b_1 \geq 2^{n-1}+1$

$2^{n-1} < a_1 b_1 - 1 = x^3 \leq 2^{2n} - 1 < 2^{2n}$

$\Rightarrow 2^{\frac{n-1}{3}} < x \leq 2^{\frac{2n}{3}}$

13 Enunciado B Sección 2.4

6 Si Tenemos

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

y $\gcd(x+1, x^2-x+1)$

$= \gcd(x+1, x^2-x+1 - x(x+1))$

$= \gcd(x+1, x^2-x+1-x^2-x)$

$= \gcd(x+1, -2x+1)$

$= \gcd(x+1, -2x+1+2(x+1))$

$= \gcd(x+1, -2x+1+2x+3)$

$= \gcd(x+1, 3)$

que es 1 ó 3.