FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

CONGRUENCIAS OLÍMPICAS

Marcos Arias Fernández

Curso Académico: 2021/2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

CONGRUENCIAS OLÍMPICAS

Marcos Arias Fernández

Setembro, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Congruencias olímpicas
Breve descrición do contido
Trátase de facer unha revisión dos principais conceptos sobre congruencias que aparecen nos problemas das distintas fases da Olimpíada Matemática Española (sistemas de números congruentes, Teorema pequeno de Fermat, Teorema de Euler, Teorema de Wilson, ecuacións polinómicas módulo un primo, teorema chinés dos restos, raíces primitivas, criterios de divisibilidade, etc.), facer unha recollida de enunciados e presentar unha escolma de problemas resoltos.
Recomendacións
Outras observacións

Índice xeral

Resumo VII

Introdución IX

1. Congruencias **1**

1.1. Conceptos iniciais 1

1.2. Criterios de divisibilidade 4

2. Congruencias de primeiro grao **7**

2.1. Teoremas iniciais 7

2.2. Resolución de congruencias de primeiro grao 12

3. Problemas **21**

3.1. Olimpíadas Matemáticas nacionais 22

3.2. Olimpíada matemática internacional 26

3.3. Outros problemas 29

Bibliografía **33**

Resumo

No presente traballo de fin de grao tratarase de dar un contexto teórico a determinados problemas das Olimpíadas Matemáticas, ademais de presentar solución a unha selección deles.

Na parte teórica tratarase de definir que é unha congruencia, como resolver as congruencias e sistemas de congruencias de primeiro grao.

Na práctica resolveranse problemas de congruencias das Olimpíadas Matemáticas a niveis nacionais e internacionais ademais de algúns problemas de interese.

Abstract

The present final degree project will give a theorical context to some of the olympiad problems, It will also present a solution to a selection of them.

In the theoretical part It will be defined what a congruence is, how first degree congruences and systems can be solved.

In the practical part some problems of congruences from the mathematical olympiads in a national and international levels with some other interesting problems will be solved.

Introdución

No presente traballo de fin de Grao da Facultade de Matemáticas na USC, tratarase de dar contexto teórico aos problemas de congruencias das Olimpíadas Matemáticas, para que os aspirantes teñan as ferramentas apropiadas para poder resolvelos. Dito contexto teórico é dado do xeito mais sinxelo posible, sen usar ferramentas demasiado avanzadas, para que así poida ser entendido por rapaces da ESO e do Bachillerato. Así evitouse tratar temas como a teoría de grupos xa que non resultan razoables para eses niveis, ademais de resultar pouco útil para a resolución dos posibles problemas que teñan que afrontar.

A teoría de congruencias foi inicialmente formulada por Johann Carl Friedrich Gauss no seu libro Disquisitiones Arithmeticae partindo conceptos tan básicos como as operacións en $\mathbb{Z}$, en especial a división euclídea que tomará un protagonismo dende un principio. Grazas á simplicidade de dita teoría resulta moi atractivo o seu uso para os problemas das Olimpíadas Matemáticas xa que permite probar a intelixencia e intuición matemática de rapaces cuxa base teórica non conta con conceptos avanzados.

E notorio tamén denotar que Gauss apoiase a ombros de xigantes, así e común que lendo o libro fanse referencia a outros autores, un dos mais importantes é Leonhard Paul Euler, ao que cualifica de "xenial" [2] e que da pé, entre outras cousas, á resolución das congruencias e sistemas de congruencias de primeiro grao, cuestións que son moi importantes á hora de afrontar o desafío que supoñen as Olimpíadas Matemáticas.

Neste traballo ademais é moi importante a estimulación da creatividade e enxeño do aspirante, xa que, como se poden observar nos problemas resoltos, requiren o uso dos coñecementos adquiridos de xeito creativo e, polo tanto, ter un coñecemento realmente profundo das propiedades aquí descritas.

Se vas a participar en ditas Olimpíadas, xa sexa a nivel local, nacional ou in-

ternacional, sería recomendable que leas atentamente e entendas ben os problemas resoltos e trates de resolvelos todos, inclusive os xa resoltos, tratando de esquecer a resolución presentada, xa que moitos destes problemas teñen múltiples solucións, e, polo tanto, poderás estimular ese coñecemento matemático ás veces escondido por falta de adestramento. Este é ao fin e ao cabo o espírito das Olimpíadas Matemáticas.

Capítulo 1

Congruencias

1.1. Conceptos iniciais

Definición 1.1. Unha relación é un subconxunto do produto cartesiano de un ou máis conxuntos. [1]

Proposición 1.2. *Podemos clasificar as relacións acorde a cantos conxuntos interveñen:*

- *unitaria: Dicese daquela na que intervén só un conxunto.*
- *binaria: Dicese daquela na que interveñen dous conxuntos.*
- *n-aria: Dicese daquela na que interveñen n conxuntos.*

[1]

Exemplo 1.3. Sexa $A = \{a, b, c\}$ e $B = \{1, 2, 3, 4\}$ unha posible relación binaria será $R = \{(a, 1), (a, 2), (c, 4)\}$.

Exemplo 1.4. Sexa $\mathbb{N}$ o conxunto dos números naturais. Definimos a relación unitária $R = \{2n \text{ para todo } n \in \mathbb{N}\}$ que estabelece a relación de paridade.

Definición 1.5. Dicemos que R é unha relación de equivalencia se esta é unha relación binaria de elementos de X e ademais R cumpre as seguintes propriedades:

- *Reflexividade*: Para todo $x \in X$, $(x, x) \in R$.
- *Simetría*: Para todo $(x, y) \in R$ con $x, y \in X$ entón $(y, x) \in R$.

- *Transitividade*: Para todo $x, y, z \in X$, se $(x, y), (y, z) \in R$, entón $(x, y) \in R$.

[1]

Definición 1.6. O resto r de dividir a entre n con $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ denominarémolo residuo. [1]

Definición 1.7. Se $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$ dicimos que $a \equiv b \pmod{n}$, ou o que é o mesmo, a é congruente con b módulo n, se a e b teñen o mesmo residuo ao dividir entre n.

Definición 1.8. Definimos $\mathbb{Z}_n = \{0, 1, ... n-1\}$.

Teorema 1.9. *As congruencias son relacións de equivalencia, é dicir, cumpre as propiedades:*

- *Reflexividade: Para todo $x \in \mathbb{Z}$ e $n \in \mathbb{N}$, $x \equiv x \pmod{n}$.*
- *Simetría: Sexan $x,\ y \in \mathbb{Z}$ e $n \in \mathbb{N}$, se $x \equiv y \pmod{n}$ tamén cúmprese que $y \equiv x \pmod{n}$ para todo $n \in \mathbb{N}$.*
- *Transitividade: Sexan $x,\ y,\ z \in \mathbb{Z}$ e $n \in \mathbb{N}$, se $x \equiv y \pmod{n}$ e $y \equiv z \pmod{n}$, entón $x \equiv z \pmod{n}$ para todo $n \in \mathbb{N}$.*

[1]

Teorema 1.10. *$a \equiv b \pmod{n}$, se, e só se, $n \mid (b - a)$. [2]*

Demostración. Se $a \equiv b \pmod{n}$ sabemos que $a = n \cdot d_1 + r,\ b = n \cdot d_2 + r$ sendo r os residuos de a e de b, entón $b - a = n \cdot (d_2 - d_1)$.

Por outra banda, se $n \mid (b-a)$, entón $b-a = n \cdot \alpha$ e como $a = n \cdot d_1 + r_1,\ b = n \cdot d_2 + r_2$ sendo r_1 e r_2 os residuos, $b-a = n \cdot d_2 + r_2 - (n \cdot d_1 + r_1) = n \cdot (d_2 - d_1) + r_2 - r_1 = n \cdot \alpha$, polo tanto $r_2 - r_1$ é un múltiplo de n, pero como $-n < r_2 - r_1 < n$, entón $r_2 - r_1 = 0$ e, polo tanto, $r_2 = r_1$.

□

Teorema 1.11. *Podemos afirmar que para todo $a \in \mathbb{Z}$ existe un único r residuo tal que $a \equiv r \pmod{n}$ e $r \in \mathbb{Z}_n$. [1]*

Demostración. Unha das propiedades da división euclidea e que $D = d \cdot c + r$ onde D é o dividendo, d é o divisor, c é o cociente e r é o resto. Se a é o dividendo é n o divisor teríamos que $a = \alpha n + r$, entón $a - r = \alpha n$, polo tanto $a \equiv r \pmod{n}$. □

Teorema 1.12. *Sexan $x, y, z, q \in \mathbb{Z}$, $n \in \mathbb{N}$ e temos que $x \equiv y \pmod{n}$ e $z \equiv q \pmod{n}$, entón $x + z \equiv y + q \pmod{n}$. [2]*

Demostración. Como $x \equiv y \pmod{n}$, tense que $x - y \equiv 0 \pmod{n}$; e ademais como $z \equiv q \pmod{n}$, tamén temos que $z - q \equiv 0 \pmod{n}$, entón $(x-y)+(z-q) = (x+z)-(y+q) \equiv 0 \pmod{n}$ e, polo tanto, $x + z \equiv y + q \pmod{n}$. □

Teorema 1.13. *Sexan $x \equiv y \pmod{n}$ e $z \equiv q \pmod{n}$. Entón $xz \equiv yq \pmod{n}$; $x, y, z, q \in \mathbb{Z}$, $n \in \mathbb{N}$. [2]*

Demostración. Como $x \equiv y \pmod{n}$, entón $z \cdot x \equiv z \cdot y \pmod{n}$ e ademais sabemos que $z \equiv q \pmod{n}$, entón $z \cdot y \equiv q \cdot y \pmod{n}$. Agora aplicando a propriedade transitiva das relacións de equivalencia deducimos que $x \cdot z \equiv q \cdot y \pmod{n}$. □

Corolario 1.14. *Se $x \equiv y \pmod{n}$, entón $x^a \equiv y^a \pmod{n}$; para todo $a \in \mathbb{N}$. [2]*

Demostración. Basta con observar que a como $x \equiv y \pmod{n}$ podemos dicir polo teorema anterior que $\underbrace{x \cdot x \cdot \ldots \cdot x}_{a \text{ elementos}} = \underbrace{y \cdot y \cdot \ldots \cdot y}_{a \text{ elementos}} \Longleftrightarrow x^a \equiv y^a \pmod{n}$. □

Teorema 1.15. *Se $x \equiv y \pmod{n}$ e x, y, n divisibles entre α onde $x = a \cdot \alpha$, $y = b \cdot \alpha$ e $n = m \cdot \alpha$, entón $a \equiv b \pmod{m}$.*

Demostración. Basta con ver que se $x \equiv y \pmod{n}$, entón $y - x = \beta \cdot n$, entón $b \cdot \alpha - a \cdot \alpha = \alpha \cdot (b - a) = \beta \cdot \alpha \cdot m$, entón $b - a = \beta \cdot m$. □

Teorema 1.16. *Se $x \equiv y \pmod{n}$, $A_1 \equiv \alpha_1 \pmod{n}$, $A_2 \equiv \alpha_2 \pmod{n}$,...,$A_m \equiv \alpha_m \pmod{n}$, $m \in \mathbb{N}$, entón $A_1x^{a_1}+A_2x^{a_2}+\ldots+A_mx^{a_m} \equiv \alpha_1y^{a_1}+\alpha_2y^{a_2}+\ldots+\alpha_my^{a_m} \pmod{n}$; para todo $n \in \mathbb{N}$. [2]*

Demostración. Consecuencia directa de aplicar os teoremas anteriores. □

1.2. Criterios de divisibilidade

Como regra xeral para deducir os criterios de divisibilidade basta con observar que os números da forma $a_n a_{n-1} ... a_1 a_0$ se poden escribir da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ e usar axeitadamente as propiedades anteriores, en especial é necesario ver con que número é congruente o 10 e as súas sucesivas potencias.

A continuación veranse algúns exemplos.

Teorema 1.17 (Congruencia módulo 2)**.** *Todo número é congruente coa súa cifra das unidades módulo* 2*.*

Demostración. Tomemos o número $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$, entón como $10 \equiv 0 \pmod 2$, $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv a_0 \pmod 2$. □

Exemplo 1.18. $3427 \equiv 7 \equiv 1 \pmod 2$

Teorema 1.19 (Congruencia módulo 3)**.** *Tódo número é congruente coa suma de todas as súas cifras en módulo* 3*.*

Demostración. Tomemos o número $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$. Como $10 \equiv 1 \pmod 3$, entón $10^n \equiv 1^n = 1 \pmod 3$, entón $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv a_n \cdot 1 + a_{n-1} \cdot 1 + ... + a_1 \cdot 1 + a_0 = a_n + a_{n-1} + ... + a_1 + a_0 \pmod 3$. □

Exemplo 1.20. $3427 \equiv 3 + 4 + 2 + 7 = 16 \equiv 7 \equiv 1 \pmod 3$.

Teorema 1.21 (Congruencia módulo 4)**.** *Todo número é congruente módulo 4 coa suma de o dobre da segunda cifra e a última.*

Demostración. Se o número é da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$, como $10 \equiv 2 \pmod 4$ e $10^i \equiv 0 \pmod 4$ para todo $i \in \mathbb{N}$, $i \geq 2$ $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv 2 \cdot a_1 + a_0 \pmod 4$. □

Exemplo 1.22. $3427 \equiv 2 \cdot 2 + 7 = 11 \equiv 3 \pmod 4$.

Teorema 1.23 (Congruencia módulo 5)**.** *Todo número é congruente coa súa última cifra módulo 5.*

Demostración. Se o número é da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$, como $10 \equiv 0 \pmod 5$, $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv a_0 \pmod 5$. □

Exemplo 1.24. $3427 \equiv 7 \equiv 2 \pmod 5$.

Teorema 1.25 (Congruencia módulo 6)**.** *Todo número da forma* $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ *é congruente con* $\sum_{i=0}^{n}[(-2)^i \mod 6] \cdot a_i$ *módulo 6.*

Demostración. Se o número é da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$, como $10 \equiv -2 \pmod 6$, polo tanto $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv \sum_{i=0}^{n}[(-2)^i \mod 6] \cdot a_i \pmod 6$. □

Exemplo 1.26. $3427 \equiv (-2) \cdot 3 + 4 \cdot 4 + (-2) \cdot 2 + 7 = -6 + 16 - 4 + 7 \equiv 13 \equiv 1$ (mód 6).

Teorema 1.27 (Congruencia módulo 7)**.** *Todo número da forma* $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ *é congruente con* $3 \cdot (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_1 - 2 \cdot a_0) \pmod 7$*. E se queremos comprobar se a é divisible entre 7 basta con ver se* $a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_1 - 2 \cdot a_0 \equiv 0 \pmod 7$.

Demostración. Se o número é da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$, como $10 \equiv 3 \pmod 7$ e $1 \equiv -6 \pmod 7$, entón $10 \cdot (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_1) + a_0 \equiv 3 \cdot (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_1 - 2 \cdot a_0) \pmod 7$. Ademais, no caso de que o número sexa divisible entre 7, como temos que $3 \cdot (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_1 - 2 \cdot a_0) \equiv 0 \pmod 7$, como 7 non divide a 3 temos que 7 divide a $a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_1 - 2 \cdot a_0$, polo tanto $a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_1 - 2 \cdot a_0 \equiv 0 \pmod 7$. □

Exemplo 1.28. Vexamos se 3427 é múltiplo de 7. $342 - 2 \cdot 7 = 328$, $32 - 2 \cdot 8 = 16 \equiv 2$ (mód 7), polo que non é múltiplo de 7.

Exemplo 1.29. Vexamos se 23989 é múltiplo de 7. $2398 - 2 \cdot 9 = 2380$, $23 - 16 = 7 \equiv 0 \pmod 7$, polo que é múltiplo de 7.

Teorema 1.30 (Congruencia módulo 8)**.** *Todo número da forma* $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ *é congruente con* $4 \cdot a_2 - 2 \cdot a_1 + a_0$ *módulo 8.*

Demostración. Se o número é da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$, como $10 \equiv -2 \pmod 8$, entón $10^2 \equiv 4 \pmod 8$ e $10^i = 10^3 \cdot 10^{i-3} \equiv 0 \pmod 8$ para todo $i \in \mathbb{N}$, entón $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv 4 \cdot a_2 - 2 \cdot a_1 + a_0 \pmod 8$. □

Exemplo 1.31. $3427 \equiv (-2)^2 \cdot 4 + (-2) \cdot 2 + 7 = 16 - 4 + 7 \equiv 7 \equiv 1 \pmod 3$.

Teorema 1.32 (Congruencia módulo 9)**.** *Todo número da forma* $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ *é congruente con* $\sum_{i=0}^{n} a_i$ *módulo 9.*

Demostración. Se o número é da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$, como $10 \equiv 1 \pmod 9$, entón $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv \sum_{i=0}^{n} a_i \pmod 9$. □

Exemplo 1.33. $3427 \equiv 3 + 4 + 2 + 7 = 16 \equiv 7 \pmod 9$.

Teorema 1.34 (Congruencia módulo 10)**.** *Todo número da forma* $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ *é congruente con* a_0 *módulo 10.*

Demostración. Se o número é da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ como $10 \equiv 0 \pmod{10}$, entón $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv a_0 \pmod{10}$. □

Exemplo 1.35. $3427 \equiv 7 \pmod{10}$.

Teorema 1.36 (Congruencia módulo 11)**.** *Todo número da forma* $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ *é congruente con* $\sum_{i=0}^{n} (-1)^i a_i$ *módulo 11.*

Demostración. Se o número é da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ como $10 \equiv -1 \pmod{11}$, entón $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0 \equiv \sum_{i=0}^{n} (-1)^i a_i \pmod{11}$. □

Exemplo 1.37. $3427 \equiv -3 + 4 - 2 + 7 = 16 \equiv 6 \pmod{11}$.

Capítulo 2

Congruencias de primeiro grao

2.1. Teoremas iniciais

Definición 2.1 (Divisor e múltiplo)**.** Dicimos que c é divisor de a ou a é múltiplo de c, con a e $c \in \mathbb{N}$, se $c \geq 1$ e $c \leq a$ e existe $n \in \mathbb{Z}$ tal que $a = c \cdot n$, é dicir $a \equiv 0$ (mód c).

Definición 2.2 (Números primos relativos ou coprimos)**.** Dicimos que a e b, a e $b \in \mathbb{N}$, son coprimos ou primos relativos cando non existe c divisor común a a e b distinto de 1.

Exemplo 2.3. 36 e 35 son primos relativos.

Definición 2.4 (Números primos e compostos)**.** Dicimos que p, con $p \in \mathbb{N} - \{0, 1\}$, é un número primo cando non existe c divisor de p distinto de 1 e p. No caso de que exista c distinto de 1 ou x tal que $c \mid x$, diremos que x é composto.

Definición 2.5 (Mínimo común múltiplo)**.** Diremos que M é o mínimo común múltiplo de a_1, a_2, ... , a_n se M é o menor número que é múltiplo de a_1, a_2, ... , a_n á vez.

Definición 2.6 (Máximo común divisor)**.** Diremos que m é o máximo común divisor de a_1, a_2, ... , a_n ou $(a_1, a_2, \ldots, a_n)$ se M é o maior número que é divisor de a_1, a_2, ... , a_n á vez.

Teorema 2.7 (Algoritmo de Euclides para o cálculo do máximo común divisor)**.** *Para calquera par de números* $a, b \in \mathbb{N},\ b > 0$*, tense que* $(a, b) = (a \mod b, b)$.

Demostración. Se $r = a \mod b$, tense que $a = q \cdot b + r,\ q \in \mathbb{N}$. Polo tanto, todo divisor común a b e r dividirá tamén a a, polo que $(b, r) \leq (a, b)$.

Por outra banda, dado que $r = a - q \cdot b$, todo divisor común a a e b tamén dividirá a r, polo tanto $(a, b) \leq (b, r)$.

□

Exemplo 2.8. Calculemos o máximo común divisor de 364 e 748. $(748, 364) = (748 \mod 364, 364) = (20, 364) = (20, 364 \mod 20) = (20, 4) = (20 \mod 4, 4) = (0, 4) = 4$.

Teorema 2.9 (Teorema de Bézout ou algoritmo de Euclides extendido)**.** *Para calquera par de números $a, b \in \mathbb{N}$ con algún deles distinto de 0, existen $s,\ t \in \mathbb{Z}$ tal que $(a, b) = s \cdot a + t \cdot b$*

Demostración. Sexa c o menor enteiro positivo da forma $c = x \cdot a + y \cdot b$, $x, y \in \mathbb{Z}$. Como $(a, b) \mid a,\ b$, entón $(a, b) \mid c$ e, polo tanto, $(a, b) \leq c$. Agora vexamos se $c \mid a,\ b$.

Supoñamos que $c \nmid a$, e $a = q \cdot c + r,\ 0 \leq r < c$. Entón $a > r = a - q \cdot c = (1 - q \cdot x) \cdot a + y \cdot b$, o cal non pode ser xa que a é o menor enteiro positivo que cumpre a propiedade.

□

Teorema 2.10. *Se un primo divide ao produto de dous números, entón dito primo divide a algún deses números. [2]*

Demostración. Supoñamos que $p \mid a \cdot b$ pero $p \nmid a$.E entón $a = p \cdot q + r$ con $1 \leq r \leq p - 1$, e $a \cdot b = p \cdot q \cdot b + r \cdot b$; ademais, polo teorema de Bezout temos que como $p \nmid a$, entón $(a, p) = 1 = \alpha \cdot p + \beta \cdot a$ con $\alpha,\ \beta \in \mathbb{Z}$, entón $b = \alpha \cdot p \cdot b + \beta \cdot a \cdot b$ que como $p \mid a \cdot b$ podemos afirmar que $p \mid b$.

□

Exemplo 2.11. $6 \mid 4 \cdot 21 = 84$ pero $6 \nmid 4,\ 21$.

Exemplo 2.12. $3 \mid 4 \cdot 21 = 84$ e, polo tanto, $3 \mid 4$ ou $3 \mid 21$, neste caso, $3 \mid 21$.

Corolario 2.13. *O produto de dous números distintos de 0 máis pequenos que un primo dado non pode ser múltiplo dese primo. [2]*

Teorema 2.14 (Teorema fundamental da aritmetica)**.** *Todo número enteiro ou é primo, ou se pode descompoñer de forma única, salvo orde, en factores primos. [2]*

Demostración. Primeiro observemos que ningún número natural pode poñerse como produto infinito de factores distintos a 1, xa que se así fora $m = \prod_I a_i$ con $i \in I$ e $\mid I \mid$ infinito, entón $m = \prod_I a_i \geq \prod_I 2$ o cal non pode ser un número natural porque diverxe.

Supoñamos agora que existe alo menos un número composto que se pode descompoñer en factores primos de dous ou mais xeitos. Como todo subconxunto de $\mathbb{N}$ ten que ter un mínimo, ten que existir un número composto con múltiples factorizacións en factores primos distintas que sexa o mais pequeno e denominaremolo a. Dito a terá estas duas factorizaciones primas distintas $p_1^{n_1} \cdot ... \, p_s^{n_s}$ e $q_1^{m_1} \cdot ... \, q_t^{m_t}$ con $n_1, ..., n_s, m_1, ... \, m_t \in \mathbb{N} - \{0\}$.

Sexa p primo, se $p \mid p_1^{n_1} \cdot ... \, p_s^{n_s}$, entón $p \mid q_1^{m_1} \cdot ... \, q_t^{m_t}$, polo que os primos que hai na primeira factorización teñen que ser os mesmos que os da segunda e viceversa, entón $q_1^{m_1} \cdot ... \, q_t^{m_t} = p_1^{m_1} \cdot ... \, p_s^{m_s}$. Como as factorizacións son distintas podemos supoñer sen perda de xeralidade que $n_1 < m_1$, polo que $p_2^{n_2} \cdot ... \, p_s^{n_s} = p_1^{m_1 - n_1} \cdot p_2^{m_2} \cdot ... \, p_s^{m_s} = a/p^{n_1} < a$ o cal non pode ser xa que a é o menor número composto con múltiples factorizacións en factores primos distintas.

□

Teorema 2.15. *É equivalente dicir que M é o mínimo común múltiplo de a_1, a_2, ... , a_n a dicir que M é igual ao produto de todos os factores primos de a_1, a_2, ... , a_n elevados ao maior dos exponentes das factorizacións.*

Demostración. Que M é un múltiplo é trivial xa que basta con dividir M entre cada un dos a_i para todo $i \in \{1,2, ..., n\}$ e ver que ao facelo se cancelan todos os factores primos de a_i.

Agora témos que ver que é o menor, e para iso supoñamos que existe M' múltiplo de a_1, a_2, ... , a_n menor estricto que M. Ao factorizalo en factores primos vemos que non pode haber ningún factor distinto aos factores primos de a_1, a_2, ... , a_n xa que se así fora podes definir M'' con todos os factores primos de M' menos aqueles que non sexan factores primos de a_i para todo $i \in \{1,2, ..., n\}$ que tamén sería múltiplo de estes. Polo tanto podemos dicir que os factores primos de M' tamén están en M. Como $M' < M$ alo menos un dos factores primos de M' ten que ter exponente menor ao mesmo factor primo en M. Dito exponente do primo en M é igual ao exponente do mesmo primo para a factorización de certo a_j, polo tanto, M' non pode ser múltiplo dese a_i. □

Teorema 2.16. *É equivalente dicir que m é o máximo común divisor de a_1, a_2, ..., a_n a dicir que m é igual ao produto de todos os factores primos comúnes de a_1, a_2, ..., a_n elevados ao menor exponente.*

Demostración. Que m é un divisor é trivial xa que basta con dividir cada un dos a_i para todo $i \in \{1,2, ..., n\}$ entre m e ver que ao facelo se cancelan todos os factores primos de m.

Agora témos que ver que é o maior, e para iso supoñamos que existe m' o maior divisor de a_1, a_2, ..., a_n maior estricto que m. Ao factorizalo en factores primos vemos que non pode haber ningún factor primo distinto aos factores primos comúns de a_1, a_2, ..., a_n xa que se así fora podes non sería divisor de a_i para todo $i \in \{1,2, ..., n\}$. Polo tanto podemos dicir que os factores primos de m' tamén están en m. Como $m < m'$ un dos factores primos de m' ten que ter exponente maior ao mesmo factor primo en m. Dito exponente do primo en m é igual ao exponente do mesmo primo para a factorización de certo a_j, polo tanto, m' non pode ser divisor dese a_i. □

Teorema 2.17. *Se a_1, a_2, ..., a_n son primos relativos de α se, e só se, $a_1 \cdot a_2 \cdot ... \cdot a_n$ e α tamén son primos relativos.*

Demostración. Basta con darse conta que a factorización en factores primos de $a_1 \cdot a_2 \cdot ... \cdot a_n$ é a mesma que o produto de todos os factores primos de cada un dos a_i e, polo tanto, non haberá ningún factor primo en común con α. □

Teorema 2.18. *Se a_1, a_2, ..., a_n son primos relativos entre si e todos son divisores de α, entón $a_1 \cdot a_2 \cdot ... \cdot a_n$ tamén divide a α.*

Demostración. Basta con darse conta que a factorización en factores primos de cada un dos a_1, a_2, ..., a_n ao ser divisores de α está formada so por algúns dos factores primos con exponente menor ou igual ao de α e sen ter primos en común co resto de a_i polo feito de ser coprimo destes. Disto seguese que o produto de todos eles tamén terán os mesmos primos que α con expoñente menores ou iguais aos da factorización de dito α. □

Teorema 2.19. *Tomemos $A = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot ... \cdot a_n^{\alpha_n}$ onde todo a_i é primo. Se $A = k^s$, entón α_i divide a s para todo $i \in \{1, 2, ..., n\}$. [2]*

Demostración. Como a factorización en factores primos de A é única, k^n terá a mesma factorización. Ao factorizar k podemos observar que consta de exactamente os mesmos primos que a factorización de A, xa que se no fose así, se houbera algún primo b factor de k, b tamén sería factor primo de k^s e non de A, e se algún a_i non fora factor primo de k e por tanto tampouco o sería de k^s.

Digamos que a factorización en factores primos de k é $k = a_1^{\alpha'_1} \cdot a_2^{\alpha'_2} \cdot ... \cdot a_n^{\alpha'_n}$, entón $k^s = a_1^{s,\cdot\alpha'_1} \cdot a_2^{s\cdot\alpha'_2} \cdot ... \cdot a_n^{s\cdot\alpha'_n}$. Polo tanto para todo $i \in \{1, 2, ..., n\}, \alpha_i = s \cdot \alpha'_i$, entón s divide a α_i.

□

Corolario 2.20. *Se $A = a_1 \cdot a_2 \cdot ... \cdot a_n$, onde todos os a_i son coprimos, e $A = k^n$. Entón $\sqrt[n]{a_i} \in \mathbb{N}$.*

Demostración. Basta con observar que os a_i, ao ser coprimos, non comparten ningún primo na súa factorización, polo que podemos aplicar o teorema anterior e observaremos que os expoñentes de cada un deses primos é divisible entre n.

□

Teorema 2.21. *Sexa A de xeito que sexa divisible entre α e β que son coprimos. Entón A será divisible entre $\alpha \cdot \beta$.*

Demostración. Basta con ver que os factores primos de α e β son distintos, polo que os expoñentes dos factores primos de $\alpha \cdot \beta$ non superarían aos de A, xa que tampouco ocorre en α nin en β.

□

Exemplo 2.22. $6,\ 4 \mid 12$ pero $6 \cdot 4 \nmid 12$.

Exemplo 2.23. $3,\ 4 \mid 12$ e como son coprimos, entón $3 \cdot 4 \mid 12$.

Corolario 2.24. *Se a e b son divisibles entre k e son a súa vez congruentes módulo n sendo k e n coprimos, entón $\frac{a}{k} \equiv \frac{b}{k} \pmod{n}$.*

Demostración. Basta con observar que se $a \equiv b \pmod{n}$, entón $a - b$ é divisible entre n e como a e b son a súa vez divisibles entre k, $a - b$ tamén o será. Polo tanto podemos aplicar o teorema anterior e concluiremos que $a - b = k \cdot n \cdot m$ para algún $m \in \mathbb{Z}$, entón $\frac{a-b}{k} = \frac{a}{k} - \frac{b}{k} = n \cdot m$, entón $\frac{a}{k} \equiv \frac{b}{k} \pmod{n}$.

□

Teorema 2.25. *Sexan α e n coprimos e sexan a e b tales que $a \not\equiv b \pmod{n}$, entón $\alpha \cdot a \not\equiv \alpha \cdot b \pmod{n}$.*

Demostración. Supoñamos nas condicións do teorema que $\alpha \cdot a \equiv \alpha \cdot b \pmod{n}$. Entón $\alpha \cdot a - \alpha \cdot b = m \cdot n$ con $m \in \mathbb{Z}$ e $\alpha \cdot (a-b) = m \cdot n$. Como α e n son coprimos, α divide únicamente a m, é dicir $\frac{m}{\alpha} = s \in \mathbb{Z}$, entón $a - b = s \cdot n$ e $a \equiv b \pmod{n}$, o cal contradice as hipóteses do teorema. □

Corolario 2.26. *Sexan $a,\ n \in \mathbb{Z}$ son coprimos, existe $x \in \mathbb{Z}$ de xeito que $a \cdot x \equiv b \pmod{n}$. Ademais sexan $x',\ x''$ tales que $a \cdot x' \equiv b \pmod{n}$ e $a \cdot x'' \equiv b \pmod{n}$, entón $x' \mod n = x'' \mod n$.*

Demostración. Definamos $R = 0, 1, \ldots n-1$ os posibles restos de dividir calquera número entre n. Supoñamos agora sen perda de xeralidade que para todo $x \in R, a \cdot x - b \not\equiv c \pmod{n}$, entón $a \cdot x \not\equiv c - b \equiv i \pmod{n}, i \in R$. Se $x_1, x_2 \in R, x_1 \neq x_2$, entón $a \cdot x_1 \not\equiv a \cdot x_2 \pmod{n}$, entón o coxunto de todos os elementos aos que equivale $a \cdot x$ vai ser exactamente R o cal non pode ser xa que non exclue a i.

□

Corolario 2.27. *A expresión $a \cdot x + b$ podemos facela congruente con calquera valor en módulo n se, e só se, a e n son coprimos.*

2.2. Resolución de congruencias de primeiro grao

Definición 2.28 (Congruencia de primeiro grao)**.** Chamamos congruencia de primeiro grao as congruencias entre polinómios de grao 1. Ditas congruencias pódense reducir de xeito trivial a $a \cdot x + b \equiv c \pmod{n}$.

Corolario 2.29. *Se a e n són coprimos a congruencia de primeiro grao $a \cdot x + b \equiv c \pmod{n}$ sempre é resoluble e a solución é única para valores de x entre 0 e $n-1$.*

Demostración. Basta con observar que sempre existe x congruente con $b - c$ módulo n. □

Teorema 2.30 (Polinomios de módulo primo)**.** *Dado o polinomio $A_n \cdot x^n + A_{n-1} \cdot x^{n-1} + \ldots A_1 \cdot x + A_0 = 0$, con $A_i \in \mathbb{Z}$ para todo $i \in \{0,\ 1, \ldots,\ n\}$, $\alpha \in \mathbb{Z}$ é solución de $A_n \cdot x^n + A_{n-1} \cdot x^{n-1} + \ldots A_1 \cdot x + A_0 = 0$ se, e só se, $\alpha \mod p$ é solución de $A_n \cdot x^n + A_{n-1} \cdot x^{n-1} + \ldots A_1 \cdot x + A_0 \equiv 0 \pmod{p}$ para todo p primo.*

Demostración. Se $x = \alpha$ é solución de $A_n \cdot x^n + A_{n-1} \cdot x^{n-1} + ... A_1 \cdot x + A_0 = 0$, entón $A_n \cdot x^n + A_{n-1} \cdot x^{n-1} + ... A_1 \cdot x + A_0 = (x - \alpha) \cdot g(x) \equiv 0 \pmod{p}$, entón $x - \alpha \equiv 0 \pmod{p}$ e $x \equiv \alpha \pmod{p}$

Por outra banda supoñamos que $x = \alpha \mod p$ é solución da congruencia $A_n \cdot x^n + A_{n-1} \cdot x^{n-1} + ... A_1 \cdot x + A_0 \equiv 0 \pmod{p}$, e sexa $\prod_{i=1}^{s}(x - a_s) \cdot g(x)$ a factorización do polinomio con todas as raíces enteiras deste. α ten que ser congruente a algunha desas raíces enteiras módulo p xa que se non fora así $g(\alpha) \equiv 0 \pmod{p}$, entón existe $a \in \mathbb{Z}$ tal que $a = p \cdot q + \alpha$, entón a é raíz de g o cal non é posible.

□

Teorema 2.31. *Se o máximo común divisor de a e n divide a $c - b$, a congruencia $a \cdot x + b \equiv c \pmod{n}$ é resoluble e ten (a, n) solucións entre 0 e $n - 1$. Non haberá solución en caso contrario. [2]*

Demostración. Sexa α o máximo común divisor de a e n, entón $a \cdot x \equiv c - b \pmod{n}$, entón $\frac{a}{\alpha} \cdot x \equiv \frac{c-b}{\alpha} \pmod{\frac{n}{\alpha}}$ que induce a unha congruencia que é resoluble cunha única solución $x_0 \in \{0, 1, ..., \frac{n}{\alpha}\}$, entón para todo $i \in \{0, 1, ... \alpha - 1\}$ $x_0 + i \cdot \frac{n}{\alpha}$ tamén serán solucións e serán todas as que se encontran entre 0 e $n - 1$.

Para ver se hai solución en caso contrario basta con supoñer que esta existe. Sexa β dita solución, polo tanto para certo $m \in \mathbb{Z}$ podemos dicir que $a \cdot \beta - (c - b) = m \cdot n$, entón $c - b = a \cdot \beta - m \cdot n$ o cal non pode ser xa que α divide a $a \cdot \beta - m \cdot n$ pero non pode dividir a $c - b$. □

Teorema 2.32 (Formulación clásica do teorema pequeno de Fermat)**.** *Se a e p son coprimos, con p primo, ou o que é o mesmo, p non divide a a, entón $a^{p-1} - 1 \equiv 0 \pmod{p}$. [2]*

Demostración. Sexa $a \in \mathbb{Z}$ e sexan $a, 2 \cdot a, ... (p - 1) \cdot a$ os primeiros $p - 1$ múltiplos. Os residuos de $a, 2 \cdot a, ... (p - 1) \cdot a$ son $1, 2, ... p - 1$, non necesariamente neste orde, polo tanto, $a \cdot 2 \cdot a \cdot ... \cdot (p-1) \cdot a = a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$, entón $a^{p-1} \equiv 1 \pmod{p}$.

□

Corolario 2.33 (Teorema pequeno de Fermat)**.** *Sexa p primo, para todo $a \in \mathbb{Z}$, $a^p - a \equiv 0 \pmod{p}$. [2]*

Demostración. Se $a = 0$ é sinxelo ver que $0^p - 0 \equiv 0 \pmod{p}$. Para o resto de casos como $a^{p-1} - 1 \equiv 0 \pmod{p}$, entón $a \cdot (a^{p-1} - 1) \equiv a \cdot 0 \pmod{p}$, entón $a^p - a \equiv 0 \pmod{p}$.

□

Exemplo 2.34. Cal é o residuo de 2^{2022} en base 11?

Como $2^{2022} = (2^{10})^{202} \cdot 2^2$ e pola versión clásica do teorema pequeno de Fermat sabemos que $2^{10} \equiv 1 \pmod{1}1$, entón $(2^{10})^{202} \cdot 2^2 \equiv 1^{202} \cdot 2^2 = 4 \pmod{11}$. Polo tanto o residuo de 2^{2022} en base 11 é 4.

Corolario 2.35. *Para p primo non divisor de a, $x = a^{p-2} \cdot (c - b)$ é solución de $a \cdot x + b \equiv c \pmod{p}$.*

Demostración. Como vimos $a^{p-1} - 1 \equiv 0 \pmod{p}$, entón $a^{p-1} \equiv 1 \pmod{p}$, entón $(c - b) \cdot a^{p-1} \equiv c - b \pmod{p}$, polo que se $x = a^{p-2} \cdot (c - b)$, entón $a \cdot x + b = a \cdot a^{p-2} \cdot (c - b) + b = a^{p-1} \cdot (c - b) \equiv c - b + b = c \pmod{p}$. □

Definición 2.36. Definimos $\mathbb{Z}_n^* = \{x \in \mathbb{N} \mid x < n, (x, n) = 1\}$, é dicir os coprimos de n menores a este.

Exemplo 2.37. $\mathbb{Z}_8^* = \{1,\ 3,\ 5,\ 7\}$

Definición 2.38. Definimos as operacións $+$ e $\cdot$ en $\mathbb{Z}_n$ de xeito que para todo $a, b\ \in \mathbb{Z}_n$ $a + b = (a + b) \mod n$ e $a \cdot b = (a \cdot b) \mod n$.

Teorema 2.39. *Sexan $a, b \in \mathbb{Z}$ temos que $(a + b) \mod n = [(a \mod n) + (b \mod n)] \mod n$ e $(a \cdot b) \mod n = [(a \mod n) \cdot (b \mod n)] \mod n$.*

Teorema 2.40. *Sexa $\mathbb{Z}_n^* = \{x \in \mathbb{N}$ tal que $x < n, (x, n) = 1\}$ e sexa a tal que $(a, n) = 1$. Entón $a \equiv b \pmod{n}$ con $b \in \mathbb{Z}_n^*$.*

Demostración. Supoñamos que $a \equiv t \pmod{n}, t \notin \mathbb{Z}_n^*$, é dicir $(t, n) = d \neq 1$, entón $a - t \equiv 0 \pmod{n}$, entón $a - t = k \cdot n, k \in \mathbb{Z}$, entón $a = k \cdot n - t$. Sexa p divisor primo de d, entón $k = k' \cdot p, n = n' \cdot p$ con $k, n' \in \mathbb{Z}$, entón p divide a a o cal é imposible.

□

Teorema 2.41. *Para todo $a, b \in \mathbb{Z}_n^*$ tense que $a \cdot b \mod n \in \mathbb{Z}_n^*$.*

Demostración. Basta con observar que $a \cdot b$ non ten divisores comúns con n.

□

Teorema 2.42. *Sexa $a \in \mathbb{Z}_n$, entón existe $b \in \mathbb{Z}_n$ tal que $a \cdot b \equiv 1 \pmod{n}$ se, e só se, $(a, n) = 1$.*

Demostración. Tomemos $a \in \mathbb{Z}_n^*$. Polo teorema de Bezout, existen $s, t \in \mathbb{Z}$ tal que $1 = a \cdot s + n \cdot t$,, entón $a \cdot s \equiv 1 \pmod{n}$. Reciprocamente como $s \cdot a \equiv 1 \pmod{n}$, $s \cdot a - 1 = \alpha \cdot n$ e, polo tanto, todo divisor d de n ten que dividir a $s \cdot a - 1$, polo que $d \nmid s \cdot a$ e por tanto non divide a a.

□

Teorema 2.43. *O inverso multiplicativo existe e é único para todos os elementos de $\mathbb{Z}_n^*$.*

Demostración. A existencia xa está demostrada polo teorema anterior, para a unicidade basta con ver que para $a \in \mathbb{Z}_n^*$ sexan b e c os seus inversos multiplicativos en $\mathbb{Z}_n^*$, entón $a \cdot b - a \cdot c \equiv 0 \pmod{n}$, entón $a \cdot (b - c) \equiv 0 \pmod{n}$, entón $b - c = 0$ e, polo tanto, $b = c$.

□

Definición 2.44 (Función de Euler)**.** Chamaremos función de Euler a aquela definida do seguinte xeito:

$$\varphi \colon \mathbb{Z}^* \to \mathbb{Z}^*$$

$$\varphi \colon n \rightsquigarrow \mid \mathbb{Z}_n^* \mid$$

[2]

Exemplo 2.45. $\varphi(45) = 4 \cdot 2 \cdot 3 = 24$

Teorema 2.46. $\mid \mathbb{Z}_{p^n}^* \mid = (p-1) \cdot p^{n-1}$*, para todo p primo. [2]*

Demostración. Demostrémolo por indución:

- *Base:* Para $p^1 = p$ todo-los números menores a p son coprimos xa que se non fora así existiría $a \in \mathbb{N} : (a, p) = q, q \notin \{1, p\}$ tal que q divide a p, o cal e imposíbel. Por conseguinte hai $(p-1) \cdot p^0 = p - 1$.

- *Hipótese:* Supoñamos o teorema certo para todo p^i con $i \leq n$
- *Paso n+1:* Sabemos que todos os que son coprimos con p^n tamén o serán con p^{n+1}, de feito non haberá nin mais nin menos ate p^n xa que non poden haber números coprimos con p^{n+1} que non sexan a súa vez coprimos con p^n. Ademais fagamos contas para ver como son números hai entre p^n e p^{n+1}:

  $p^n, p^n+1, \dots, p^n+p, \dots p^n+p^2+p, \dots, p^n+p^{n-1}+\dots+p^2+p+1, \dots p^n+p^n, \dots p^n \cdot p^n - 1, p^n \cdot p^n = p^{n+1}$

  Obsérvese que os números que hai entre $t \cdot p^n$ e $(t+1) \cdot p^n$ pódense poñer da forma $t \cdot p^n + k$ con k entre 0 e p^n. Ademais para que $t \cdot p^n + k$ non sexa coprimo con p^{n+1}, $\frac{t \cdot p^n + k}{p^i} = q, q \in \mathbb{N}$, para todo $i \in \{1, \dots n\}$ se, e só se, $t \cdot p^{n-i} + \frac{k}{p^i} = q$ se, e só se, $\frac{k}{p^i} = q - t \cdot p^{n-i}$, entón $t \cdot p^n + k$ non é coprimo de p^{n+1} se, e só se, k non é coprimo de p^n, entón $t \cdot p^n + k$ é coprimo de p^{n+1} se, e só se, k é coprimo de p^n, entón entre $t \cdot p^n$ e $(t+1) \cdot p^n$ temos $(p-1) \cdot p^{n-1}$ coprimos de p^{n+1} , entón entre p^n e p^{n+1} temos $(p-1) \cdot [(p-1) \cdot p^{n-1}] = (p-1)^2 \cdot p^{n-1}$ coprimos de p^{n+1}, entón teremos un total de $(p-1) \cdot p^{n-1} + (p-1)^2 \cdot p^{n-1} = (p-1) \cdot p^n$, polo que quedaría demostrado.

□

Corolario 2.47. *Se $a = p_1^{s_1} \cdot \dots \cdot p_n^{s_n}$ factorización en factores primos de, entón $\varphi(a) = \prod_{i=1}^{n} (p_i - 1) \cdot p_i^{s_i - 1}$. [2]*

Teorema 2.48 (Teorema chinés dos restos)**.** *Sexan $n_1, n_2, \dots n_s \in \mathbb{N}$ coprimos dous a dous e $a_1, a_2, \dots a_s \in \mathbb{Z}$ Existe $x \in \mathbb{Z}$:*

$$\begin{cases} x \equiv a_1 & (\text{mód } n_1) \\ \vdots & \\ x \equiv a_s & (\text{mód } n_s) \end{cases}$$

E dito x será único para $x \in \mathbb{Z}_n$ sendo $n = n = n_1 \cdot n_2 \cdot \dots \cdot n_s$ e calquera outra solución será congruente con x módulo n. [2]

Demostración. Sexa $n_i' = n/n_i$ de xeito que $(n_i', n_i) = 1$, entón $n_i' \in Z_{n_i}^*$, entón existe $m_i' \in Z_{n_i}^*$ tal que $m_i' \cdot n_i' \equiv 1 \pmod{n_i}$, entón $m_i' \cdot n_i' \cdot a_i \equiv a_i \pmod{n_i}$. Obsérvese

ademais que $m_i' \cdot n_i' \equiv 0 \pmod{n_j}$ para todo $j \neq i$, entón $n_i' \cdot a_i \equiv 0 \pmod{n_j}$ para todo $j \neq i$, entón $x = \sum_{i=1}^{s} m_i' \cdot n_i' \cdot a_i$ será solución do sistema.

Para ver a unicidade en $\mathbb{Z}_n$ supoñamos que x e y son solucións do sistema en $\mathbb{Z}_n$, polo que sabemos que $x \equiv a_i \pmod{n_i}$ e $y \equiv a_i \pmod{n_i}$ para todo $i \in \{1, 2, \dots, s\}$, entón $x - y \equiv 0 \pmod{n)_i}$ para todo $i \in \{1, 2, \dots, s\}$, entón $x - y \equiv 0 \pmod{n}$ por ser os n_i coprimos, entón $x \equiv y \pmod{n}$ e, polo tanto, $x = y$.

□

Teorema 2.49. *Se m e n son coprimos, entón $\mid \mathbb{Z}_{m\cdot n}^* \mid = \mid \mathbb{Z}_m^* \mid \cdot \mid \mathbb{Z}_n^* \mid$. [2]*

Demostración. Para proba-lo vexamos que existe unha bixección entre $\mathbb{Z}_{m\cdot n}^*$ e $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Podemos definila deste xeito:

$$f \colon \mathbb{Z}_{m\cdot n}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$$
$$f \colon x \rightsquigarrow (x \mod m, x \mod n)$$

Vexamos primeiro que está ben definida xa que se $(x, m \cdot n) = 1$ e $(x, m) = d$, como d divide a $m \cdot n$, entón $d = 1$, analogamente tamén para n.

Probemos a inxectividade. Sexan $x, y \in \mathbb{Z}_{m\cdot n}^*$ e supoñamos que $f(x) = f(y)$, entón $x \equiv y \pmod{m}$ e $x \equiv y \pmod{n}$, entón $x - y = k \cdot m, x - y = k' \cdot n$, entón $k \cdot m = k' \cdot n$ e como m e n son coprimos, ou $x - y = m \cdot n$ o cal é imposíbel ou $x - y = 0$, polo tanto $x = y$ e quedaría demostrada a inxectividade.

Probemos agora a sobrexectividade. Tomemos $x \in \mathbb{Z}_m^*$ e $y \in \mathbb{Z}_n^*$. Polo teorema chinés dos restos, existe solución ao sistema definido do seguinte xeito:

$$\begin{cases} z \equiv x \pmod{m} \\ z \equiv y \pmod{n} \end{cases}$$

Terá solución única en $\mathbb{Z}_{m\cdot n}^*$ xa que $(m, n) = 1$. Polo tanto cúmprese a sobrexectividade. □

Corolario 2.50. *A función φ de Euler é reprodutiva respecto ao produto de coprimos de xeito que $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ se, e só se, $(m, n) = 1$. [2]*

Exemplo 2.51. $\varphi(18) = \mid \{1, 5, 7, 11, 13, 17\} \mid = 6$, ademais $\varphi(9) = 3 \cdot 2$ e $\varphi(2) = 1$. Polo tanto $\varphi(18) = \varphi(2) \cdot \varphi(9)$.

Exemplo 2.52. $\varphi(36) = \mid \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} \mid = 12$, ademais $\varphi(9) = 3 \cdot 2$ e $\varphi(4) = 1 \cdot 2$. Polo tanto $\varphi(36) = \varphi(4) \cdot \varphi(9)$.

Teorema 2.53. *Sexa $a \in \mathbb{Z}$ tal que $(a, n) = 1$, entón $a \cdot \mathbb{Z}_n^* = \{a \cdot x \mod n$ para todo $x \in \mathbb{Z}_n^*\} = \mathbb{Z}_n^*$.*

Demostración. Que $a \cdot x \in \mathbb{Z}_n^*$ xa está demostrado. Como $\mathbb{Z}_n^*$ é un conxunto finito basta con ver que pasa para $x, y \in \mathbb{Z}_n^*$ tal que $a \cdot x \equiv a \cdot y \pmod{n}$, entón $a \cdot (x - y) \equiv 0 \pmod{n}$, entón $x \equiv y \pmod{n}$, entón $x = y$. polo que $a \cdot \mathbb{Z}_n^*$ e $\mathbb{Z}_n^*$ teñen a mesma cantidade de elementos e, polo tanto, son o mesmo conxunto.

□

Teorema 2.54 (Teorema de Euler)**.** *Se a e n son coprimos, entón $a^{\varphi(n)} \equiv 1$ (mód n). [2]*

Demostración. Sexa $a' \in \mathbb{Z}_n^*$ tal que $a \equiv a' \pmod{n}$. Definamos agora $\prod_{z \in \mathbb{Z}_n^*} z$, do cal podemos afirmar que $\prod_{z \in \mathbb{Z}_n^*} z \equiv \prod_{z \in \mathbb{Z}_n^*} a' \cdot z \pmod{n}$, entón $a'^{\varphi(n)} \cdot \prod_{z \in \mathbb{Z}_n^*} z \equiv \prod_{z \in \mathbb{Z}_n^*} z$, entón $a'^{\varphi(n)} \equiv 1 \pmod{n}$, entón $a^{\varphi(n)} \equiv 1 \pmod{n}$.

□

Exemplo 2.55. $(2, 21) = 1$, polo tanto 20 e 21 son coprimos. $2^{\varphi(21)} = 2^{6 \cdot 2} = 2^1 2 = 4096 = 195 \cdot 21 + 1$, entón $2^{\varphi(21)} \equiv 1 \pmod{21}$.

Definición 2.56. Chamamos orde de a en n, $Ord_n(a)$, ao menor enteiro positivo tal que $a^{Ord_n(a)} \equiv 1 \pmod{n}$.

Exemplo 2.57. Vexamos canto vale $2^i \mod 21$ ate o menor i natural distinto de 0 que se faga que $2^i \equiv 1 \pmod{21}$: $2,\ 4,\ 8,\ 16,\ 11,\ 1$, entón $Ord_{21}(2) = 6$.

Teorema 2.58. *Sexa $a \in \mathbb{Z}_n^*$, entón $Ord_n(a) \mid \varphi(n)$.*

Demostración. Por definición sabemos que $t = Ord_n(a)$ cumpre que $t \leq \varphi(n)$. Supoñamos que o resultado non é certo, é dicir $\varphi(n) = t \cdot q + r$ con $q, r \in \mathbb{N}, 1 < r < t$, entón $a^{\varphi(n)} = a^{t \cdot q} \cdot a^r \equiv a^r \equiv 1 \pmod{n}$ o cal non pode ser certo xa que $r < t$.

□

Exemplo 2.59. $\varphi(21) = 12$ e $Ord_{21}(2) = 6$, entón pode observarse que $Ord_{21}(2) \mid \varphi(21)$.

Corolario 2.60. *$a^t \equiv 1 \pmod{n}$ se, e só se, $Ord_n(a) \mid t$.*

Demostración. Se supoñemos que $Ord_n(a) \mid t$ a demostración é trivial.

Supoñamos por outra banda que $a^t \equiv 1 \pmod{n}$ pero $Ord_n(a) \nmid t$. Basta con realizar un argumento similar ao teorema anterior para chegar á contradición.

□

Teorema 2.61 (Solución de congruencias de primeiro grao)**.** *Sexa a congruencia de primeiro grao* $a \cdot x \equiv b \pmod{n}$*. Dita congruencia terá algunha solución se, e só se,* $(a,n) \mid b$*, e ditas solucións serán* $x = (\frac{a}{(a,n)})^{\varphi(n/(a,n))-1} \cdot (b/(a,n)) + k \cdot \frac{n}{(a,n)} \bmod n,\ k \in \{0,1,\dots (a,n)-1\}$ *en* $\mathbb{Z}_n$

Demostración. Xa estamos en condicións de dar solución as congruencias de primeiro grao. Sexa $d = (a,n), a' = a/d, b' = b/d$ e $n' = n/d$, polo que resolver $a \cdot x \equiv b \pmod{n}$ é equivalente a resolver $a' \cdot x \equiv b' \pmod{n'}$. Ademais a solución de $a' \cdot x \equiv 1 \pmod{n'}$ será $a'^{\varphi(n')-1}$ xa que $a'^{\varphi(n')} = a \cdot a'^{\varphi(n')-1} \equiv 1 \pmod{n'}$, entón $a \cdot (a'^{\varphi(n')-1} \cdot b') \equiv b' \pmod{n)'}$ e, polo tanto, $a'^{\varphi(n')-1} \cdot b' + k \cdot n'$ para todo $k \in \mathbb{Z}$ será solución tamén de $a \cdot x \equiv b \pmod{n}$.

Vexamos que $a'^{\varphi(n')-1} \cdot b' + k \cdot n', k \in \{0,1,\dots (a,n)-1\}$ son solucións distintas en $\mathbb{Z}_n$.É trivial comprobar que son solución, agora supoñamos que para $k', k'' \in \{0,1,\dots (a,n)-1\}, a'^{\varphi(n')-1} \cdot b' + k' \cdot n' \equiv a'^{\varphi(n')-1} \cdot b' + k'' \cdot n' \pmod{n}$, entón $k' \cdot n' \equiv k'' \cdot n' \pmod{n}$, entón $k' \equiv k'' \pmod{d}$, entón $k' = k''$ o cal non pode ser certo.

Vexamos que non pode haber ningunha solución en $\mathbb{Z}_n$ que non sexa da forma $a'^{\varphi(n')-1} \cdot b' + k \cdot n' \bmod n,\ k \in \{0,1,\dots (a,n)-1\}$. Supoñamos que z é unha solución en $\mathbb{Z}_n$ distinta a $a'^{\varphi(n')-1} \cdot b' + k \cdot n', k \in \{0,1,\dots (a,n)-1\}$, entón $a \cdot z \equiv a \cdot a'^{\varphi(n')-1} \cdot b' \pmod{n}$, entón $a' \cdot z \equiv 1 \pmod{n'}$. Como $a' \in \mathbb{Z}^*_{n'}$ sabemos, polo tanto, que ten inversa e é única, e esta é $a'^{\varphi(n')-1}$ que non lle queda outra a z que tomar ese valor.

□

Exemplo 2.62. Sexa $6 \cdot x \equiv 9 \pmod{21}$, entón $(6,21) = 3$, polo que $2 \cdot x \equiv 3 \pmod{7}$ e a súa solución é $x = 2^5 \cdot 3$ e por conseguinte as solucións de $6 \cdot x \equiv 9 \pmod{21}$ son $x = 2^1 1 \cdot 3 + k \cdot 7 \bmod 21$ para $k \in \{0,1,2\}$, entón comprobemos que $12,\ 19,\ 5$ son solucións: $6 \cdot 12 \bmod 21 = 72 \bmod 21 = 9$, $6 \cdot 19 \bmod 21 = 114 \bmod 21 = 9$ e $6 \cdot 15 \bmod 21 = 30 \bmod 21 = 9$

Corolario 2.63. *A solución de* $a \cdot x \equiv b \pmod{n}$ *con* $(a,n) \mid b$ *é* $x = (\frac{a}{(a,n)})^{Ord_{n/(a,n)}(a)-1} \cdot (b/(a,n)) + k \cdot \frac{n}{(a,n)} \bmod n,\ k \in \{0,1,\dots (a,n)-1\}$

Exemplo 2.64. No exemplo anterior as solucións son da forma $x = 2^2 \cdot 3 + k \cdot 7 \mod 21$ para $k \in \{0, 1, 2\}$, o que da como solucións $12,\ 19,\ 5$.

Teorema 2.65 (Sistemas de congruencias de primeiro grao)**.** *Sexa un sistema de congruencias de primeiro grao da forma:*

$$\begin{cases} x \equiv a_1 & (\text{mód } n_1) \\ \quad \vdots & \\ x \equiv a_s & (\text{mód } n_s) \end{cases}$$

Podemos obter a solución se esta existe, e esta estará garantida se o módulos son coprimos dous a dous.

Demostración. Que a existencia está garantida se os módulos son coprimos polo teorema chinés dos restos.

Para ver os casos nos que hai solución basta con observar o algoritmo de resolución.

Da primeira congruencia podemos deducir que $x = a_1 + k_1 \cdot n_1$, e utilizando isto na seguinte obtemos que $a_1 + k_1 \cdot n_1 \equiv a_2 \pmod{n_2}$ que terá solución se (n_1, n_2) divide a $a_2 - a_1$.

Iterando o proceso, ao resolver a última congruencia obterase a solución sempre que se cumpra a condición arriba descrita.

□

Exemplo 2.66. Resolvamos:

$$\begin{cases} x \equiv 3 & (\text{mód } 4) \\ x \equiv 5 & (\text{mód } 9) \end{cases}$$

Como $x \equiv 3 \pmod 4$ entón $x = 4 \cdot q_1 + 3$. E como $x \equiv 5 \pmod 9$ temos que $4 \cdot q_1 + 3 \equiv 5 \pmod 9$, entón $4 \cdot q_1 \equiv 2 \pmod 9$ e como $Ord_9(4) = 3$, entón $q_1 = 4^2 \cdot 2$, e, polo tanto, $x = 4 \cdot 4^2 \cdot 2 + 3 = 131$

Capítulo 3

Problemas

Introduciomos aquí unha selección de problemas extraídos das Olimpíadas Matemáticas a niveles locais, nacionais e internacionais, ademais de algúns problemas de interese. Respecto as Olimpíadas Matemáticas a nivel local e nacional, extraense de multiples paises, como a Unión Sovietica o Estados Unidos e, especialmente, as Olimpíadas Matemáticas Españolas.

A hora de afrontar as Olimpíadas Matemáticas Españolas deberase ter en conta a estructura:

- *Fase local, de distrito ou fase autonómica:* Celebrase ao final do primeiro trimestre en cada Comunidade Autónoma ou Distrito Universitario e consta dun total de 6 problemas repartidos en duas probas escritas. Os participantes deberán estar cursando a ensinanza secundaria e poderán presentarse voluntariamente sen requisito previo.

- *Fase Nacional:* Celebrase a finais de febreiro e consta dun total de 6 problemas comprendidos en duas probas escritas de 3 horas de duración cada unha. Cada unha destas probas constan de 3 problemas, é dicir, un total de 6 propostos por un tribunal.

Por outra banda se o aspirante vaise a enfrentar ás Olimpíadas Matemáticas internacionais, debe saber que celébranse a mediados de Xullo e consta de duas probas de 4 horas de duración cada unha, tendose que enfrentar o aspirante a un total de 6 problemas repartidas en 3 problemas por proba. [6]

3.1. Olimpíadas Matemáticas nacionais

Problema 3.1 (Olimpíada Matemática Española (OME) 2004 Problema 9). Achar todas las formas de expresar 2003 como la suma dos cadrados dos números enteiros. [4]

Solución

Sexa $x^2,\ y^2$ cadrados perfectos e como $x,\ y \equiv \{0,1,2,3\} \pmod 4$, entón $x^2,\ y^2 \equiv \{0,1\}$, polo tanto $x^2+y^2 \equiv \{0,1,2\}$. Como $2003 \equiv 3 \pmod 4$, entón $x^2+y^2 \neq 2003,$ para todo $x,\ y \in \mathbb{Z}$

Problema 3.2 (All Soviet Union Mathematical Olympiad 1970 Problema 13). Se os números que van de 11111 ao 99999 colócase en algún orde formando un número de 444445 cifras, demostrar que dito número non é unha potencia de 2. [4]

Solución

Sexan $S_1, \ldots, S_{88889}$ todos os números que van do 11111 ao 99999 de xeito que $N = \sum_{i=1}^{88889} 10^{5\cdot(i-1)} \cdot S_i$. Obsérvese que $10^5 - 1 = 99999 = 9 \cdot 11111$, entón $10^5 \equiv 1 \pmod{11111}$, é dicir, $N \equiv \sum \sum_{i=1}^{88889} S_i \pmod{11111}$. Obsérvese ademais que, por ser 11111 primo, todo elemento de $\mathbb{Z}_{11111}$ ten inversa coa suma. Ademais obsérvese que os restos dos números do 11111 ao 99999 recorren exactamente 9 veces todos os elementos de $\mathbb{Z}_{11111}$, polo tanto $N \equiv 0 \pmod{11111}$ e, polo tanto, non pode ser potencia de 2.

Problema 3.3 (OME fase local 2004 Problema 4). Existe algunha potencia de 2 tal que ao escribila no sistema decimal teña todos os seus díxitos distintos de cero e sexa posible reordenar os mesmos para formar con eles outra potencia de 2? [4]

Solución

Sexan A e B potencias de 2 tales que cumpren as condicións do problema. Se $A < B$ teremos que ou $B = 2 \cdot A$ ou $B = 4 \cdot A$ ou $B = 8 \cdot A$ xa que como todas as cifras teñen que ser distintas de 0, A e B, teñen que ter o mesmo número de cifras significativas. Ademais como os seus díxitos son os mesmos, $A \equiv B \pmod 9$, entón $B - A \equiv 0 \pmod 9$, entón $A \equiv 0 \pmod 9$ ou $3 \cdot A \equiv 0 \pmod 9$ ou $7 \cdot A \equiv 0 \pmod 9$ e ningún destes casos son posibles.

Problema 3.4 (United States Mathematical Olympiad junior 2011 Problema 1). Achar todos os números naturais tales que $2^n + 12^n + 2011^n$ é un cadrado perfecto. [4]

Solución

Se $n = 0$ temos que $2^0 + 12^0 + 2011^0 = 3$ o cal non é un cadrado perfecto. Para $n = 1$ temos que $2^1 + 12^1 + 2011^1 = 2025 = 45^2$.

Vexamos agora para $n > 1$. $2^n + 12^n + 2011^n \equiv (-1)^n + 0 + 1 \pmod 3$, é dicir, se n par $2^n + 12^n + 2011^n \equiv 2 \pmod 3$ e se n impar $2^n + 12^n + 2011^n \equiv 0 \pmod 3$, polo tanto para que a expresión sexa un cadrado perfecto, n ten que ser impar xa que $x^2 \equiv \{0,\ 1\} \pmod 3$. Ademais $2^n + 12^n + 2011^n \equiv (2)^n + 0 + 1 \pmod 4$, é dicir, se $n > 1$, $2^n + 12^n + 2011^n \equiv 3^n \pmod 4$ que sendo n impar temos que $2^n + 12^n + 2011^n \equiv 3 \pmod 4$, pero como $x^2 \equiv \{0,\ 1\} \pmod 4$ non existe $n > 1$ para o cal $2^n + 12^n + 2011^n$ é un cadrado perfecto.

Problema 3.5 (OME 1965 Problema 2). Un número de tres cifras escríbese xyz no sistema de base 7 e zyx no sistema de base 9. Cal é ese número? [7]

Solución

Se temos que xyz escribese en base 7, teremos que o número en base 10 será $x \cdot 7^2 + y \cdot 7 + z$. Do mesmo xeito como o mesmo número en base 9 é zyx, será en base 10 $z \cdot 9^2 + y \cdot 9 + x$. Polo tanto $x \cdot 7^2 + y \cdot 7 + z = z \cdot 9^2 + y \cdot 9 + x$, entón $80 \cdot z + 2 \cdot y - 48 \cdot x = 0$, entón $40 \cdot z + y - 24 \cdot x = 0$ e, polo tanto, $8 \cdot (3 \cdot x - 5 \cdot z) = y$.

Ademais obsérvese que $8 \cdot (3 \cdot x - 5 \cdot z) \equiv y \pmod 9$, entón $5 \cdot z - 3 \cdot x \equiv y \pmod 9$, entón $5 \cdot z - y \equiv 3 \cdot x \pmod 9$, polo tanto $5 \cdot z - y$ é un múltiplo de 3, entón $5 \cdot z - y \equiv 0 \pmod 3$ e, polo tanto, $y + z \equiv 0 \pmod 3$, entón ou $y + z \equiv 0 \pmod 9$ ou $y + z \equiv 3 \pmod 9$ ou $y + z \equiv 6 \pmod 9$ así que distingamos casos:

- Se $y + z \equiv 0 \pmod 9$, entón $3 \cdot x \equiv 6 \cdot z \pmod 9$, entón $x \equiv 2 \cdot z \equiv y \pmod 3$. Como $0 \leq x, y, z \leq 6$ temos que se $x = y$, $x = y + 3$ se $0 \leq y \leq 3$ ou $y = x + 3$ se $0 \leq x \leq 3$.

  Se $x = y$, entón $40 \cdot z = 23 \cdot x$, entón $x = y = z = 0$.

  Se $x = y + 3$, entón $40 \cdot z = 23 \cdot x + 3$ que no ten solución natural para $x \in \{3, 4, 5, 6\}$.

  Se $y = x + 3$, entón $40 \cdot z = 23 \cdot x - 3$ que no ten solución natural para $x \in \{3, 4, 5, 6\}$.

- Se $y + z \equiv 3 \pmod 9$, entón $3 \cdot x \equiv 6z + 3 \pmod 9$, entón $x \equiv 2 \cdot z + 1 \equiv y + 1 \pmod 3$. Como $0 \leq x, y, z \leq 6$ temos que se $x = y + 1$ se $0 \leq y \leq 5$, $x = y + 4$ se $0 \leq y \leq 2$ ou $y = x + 2$ se $0 \leq x \leq 4$.

se $x = y + 1$ non ten solución en ningún caso.

se $x = y + 4$ non ten solución en ningún caso.

se $y = x + 2$ non ten solución en ningún caso.

- Se $y+z \equiv 6 \pmod 9$, entón $3 \cdot x \equiv 6z+6 \pmod 9$, entón $x \equiv 2 \cdot z+2 \equiv y+2 \pmod 3$. Como $0 \leq x, y, z \leq 6$ temos que se $x = y + 2$ se $0 \leq y \leq 4$, $x = y + 5$ se $0 \leq y \leq 1$ ou $y = x + 1$ se $0 \leq x \leq 5$.

  se $x = y + 2$ non ten solución en ningún caso.

  se $x = y + 5$ ten solución para $y = 0$, $x = 5$ e $z = 3$.

  se $y = x + 1$ non ten solución en ningún caso.

Problema 3.6 (OME 1976 Problema 4). Demostrar que a suma de 5 cadrados perfectos consecutivos non pode ser un cadrado perfecto. [7]

Solución

A suma de cadrados perfectos consecutivos sería da forma $(n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2 = 5 \cdot n^2 + 10 = 5 \cdot (n^2 + 2)$, polo que para que esta suma sexa un cadrado perfecto es condición necesaria que $5 \mid (n^2 + 2)$, é dicir $n^2 + 2 \equiv 0 \pmod 5$. Vemos que para ningún $n \in \mathbb{Z}_5$ cúmprese a congruencia, polo que queda demostrado.

Problema 3.7 (OME 1987 Problema 3). Probar que os binomios $25 \cdot x + 31 \cdot y$ e $3 \cdot x + 7 \cdot y$ son múltiplos de 41 para os mesmos valores de x e y. [7]

Solución

Sexan a e b enteiros tales que $25 \cdot a + 31 \cdot b \equiv 0 \pmod{41}$ se, e só se, multiplicando por 2 temos que $50 \cdot a + 62 \cdot b \equiv 0 \pmod{41}$, se, e só se, $9 \cdot a + 21 \cdot b \equiv 0 \pmod{41}$ se, e só se, $3 \cdot a + 7 \cdot b \equiv 0 \pmod{41}$.

Problema 3.8 (OME 1971 Problema 7). Demostrar que para todo enteiro positivo n, o número $5^n + 2 \cdot 3^{n-1} + 1$ é múltiplo de 8. [7]

Solución

Se $n = 1$ temos que $5 + 2 + 1 = 8$ que trivialmente é un múltiplo de 8.

Para $n > 1$ impar $5^n + 2 \cdot 3^{n-1} + 1 \equiv (-3)^n + 2 \cdot 3^{n-1} + 1 \equiv 3^{n-1} \cdot [2 + (-1)^{n-1} \cdot (-3)] + 1 \pmod 8$. Como $n - 1 \geq 2$ par e $3^2 \equiv 1 \pmod 8$, entón $3^{n-1} \cdot [2 + (-1)^{n-1} \cdot (-3)] + 1 \equiv -1 + 1 \equiv 0 \pmod 8$.

Para n par $5^n + 2 \cdot 3^{n-1} + 1 \equiv (-3)^n + 2 \cdot 3^{n-1} + 1 \equiv 3^{n-1} \cdot [2 + (-1)^{n-1} \cdot (-3)] + 1$ (mód 8). Como $n-1 \geq 2$ par e $3^2 \equiv 1 \pmod 8$, entón $3^{n-1} \cdot [2+(-1)^{n-1} \cdot (-3)]+1 \equiv 3 \cdot 5 + 1 \equiv 16 \equiv 0 \pmod 8$.

Problema 3.9 (OME 1993 Problema 4). Demostrar que todo número primo distinto de 2 e 5 ten infinitos múltiplos escritos só con uns. [7]

Solución

Sexa p primo distinto de 2 e 5, polo tanto $(10^n, p) = 1$ para todo $n \in \mathbb{N}$, entón como $10^{\varphi(p)} \equiv 1 \pmod p$, entón $10^{\varphi(p)} - 1 \equiv 0 \pmod p$ ou o que é o mesmo $10^{p-1} - 1 \equiv 0 \pmod p$, entón p divide a $\underbrace{99 \cdots 9}_{p-1}$, entón para p distinto de 3 sabemos que $p \mid \underbrace{11 \cdots 1}_{p-1}$. Para $p = 3$ basta con ver que $1 + 1 + 1 \equiv 0 \pmod 3$, polo tanto $3 \mid 111$. Ademais obsérvese que para todo p primo distinto de 2, 3 e 5 $p \mid \underbrace{11 \cdots 1}_{n \cdot (p-1)}$ e $3 \mid \underbrace{11 \cdots 1}_{n \cdot 3}$, polo que queda demostrada a premisa do problema.

Problema 3.10 (OME 2002 Problema 1). Probar que para calquera primo p distinto de 2 e 5 existe un múltiplo cuxas cifras son todos noves. [7]

Solución

É unha demostración análoga ao problema anterior.

Problema 3.11 (OME Fase local 2014 Problema 2). Encontrar as 3 últimas cifras de 7^{2014}. [7]

Solución

Vexamos canto vale $7^{2014} \mod 1000$. Polo teorema de Euler, como 7 e 1000 son coprimos, temos que $7^{\varphi(1000)} \equiv 1 \pmod{1000}$, como $1000 = 2^3 \cdot 5^3$ temos que $\varphi(1000) = 2^2 \cdot 4 \cdot 5^2 = 400$, entón $7^{2014} = (7^{400})^5 \cdot 7^{14} \equiv 7^{14} = 849 \pmod{1000}$.

Polo tanto, as 3 últimas cifras de 7^{2014} són 849.

Problema 3.12 (OME 2013 Problema 6). Dado un número enteiro n escrito no sistema de numeración decimal, formamos o número enteiro k restando do número formado polas tres últimas cifras de n o número formado polas cífras anteriores restantes. Demostrar que n é divisible por 7, 11 e 13 se, e só se, k tamén o é. [7]

Solución

Sexa A o número formado polas 3 últimas cifras de n e B o número formado polas cifras restantes. Entón $n = 1000 \cdot B + A$ e $k = A - B$. Temos, polo tanto, que

$n - k = 1001 \cdot B = 7 \cdot 11 \cdot 13 \cdot B$. Polo tanto n e k son congruentes módulo 7, 11 e 13.

Problema 3.13 (OME 2012 Problema 1). Determine razoadamente se o número $\sqrt{3 \cdot n^2 + 2 \cdot n + 2}$ é irracional para todo n enteiro non negativo. [7]

Solución

Vexamos se existe a natural distinto de 0 tal que $3 \cdot n^2 + 2 \cdot n + 2 = a^2$. Como $a^2 \mod 8 \in \{0,\ 1,\ 4\}$ vexamos os valores que toma $3 \cdot n^2 + 2 \cdot n + 2 \mod 8$ respecto a n.

- $n \mod 8$=*0:* $3 \cdot n^2 + 2 \cdot n + 2 \mod 8 = 2$
- $n \mod 8$=*1:* $3 \cdot n^2 + 2 \cdot n + 2 \mod 8 = 7$
- $n \mod 8$=*2:* $3 \cdot n^2 + 2 \cdot n + 2 \mod 8 = 2$
- $n \mod 8$=*3:* $3 \cdot n^2 + 2 \cdot n + 2 \mod 8 = 3$
- $n \mod 8$=*4:* $3 \cdot n^2 + 2 \cdot n + 2 \mod 8 = 2$
- $n \mod 8$=*5:* $3 \cdot n^2 + 2 \cdot n + 2 \mod 8 = 7$
- $n \mod 8$=*6:* $3 \cdot n^2 + 2 \cdot n + 2 \mod 8 = 2$
- $n \mod 8$=*7:* $3 \cdot n^2 + 2 \cdot n + 2 \mod 8 = 3$

Polo tanto $3 \cdot n^2 + 2 \cdot n + 2$ non é un cadrado perfecto.

3.2. Olimpíada matemática internacional

Problema 3.14 (IMO shortlist 1994 Problema 24). Dicimos que un número enteiro positivo é un número ondulante se os seus díxitos en base 10 son alternativamente cero e distinto de cero, sendo o díxito das unidades distinto de cero. Determinar todos os enteiros positivos que non dividen a ningún número ondulante. [5]

Solución

É sinxelo ver que os números divisibles entre 10 e 25 non poden dividir aos números ondulantes xa que ditos números acaban en 0 e 25 respectivamente, polo tanto, nin 10 nin 25 poden dividir a ningún divisor dun número ondulante.

Vexamos o caso de que nin 2 nin 5 dividen ao candidato a divisor n: Como xa sabemos $(2, n) = (5, n) = 1$, entón $(10^k, n) = 1$, obsérvese ademais que $(10^k - 1, 10^k) = 1$ xa que se non fora así podemos tomar d divisor común de $10^k - 1$ e 10^k tal que $10^k - 1 \equiv 10^k \pmod{d}$, entón $-1 \equiv 0 \pmod{d}$ o cal é imposible. Polo teorema de Euler tense que $(10^k)^{\varphi(n)} \equiv 1 \pmod{n}$, ademais temos que $10^k - 1 \mid 10^{k\cdot\varphi(n)}$, entón $10^{k\cdot\varphi(n)} - 1 \equiv 0 \pmod{10^k - 1}$, entón $(10^k)^{\varphi(n)} - 1 = t' \cdot n$ e $(10^k)^{\varphi(n)} - 1 = t'' \cdot (10^k - 1)$ e como n e $10^k - 1$ son coprimos podemos tomar $t''' = t'/(10^k - 1)$ de xeito que $(10^k)^{\varphi(n)} - 1 = t' \cdot n = t''' \cdot (10^k - 1) \cdot n$, entón $(10^k)^{\varphi(n)} - 1 \equiv 0 \pmod{10^k - 1} \cdot n$, entón $A(k, n) = (10^k)^{\varphi(n)} - 1/10^k - 1$ é un múltiplo de n que está formado por uns separados por $k - 1$ ceros, polo que para $k = 1$ temos un número ondulante múltiplo de n.

Se $5 \mid n$ recordando que nin 10 nin 25 poden dividir a n xa que nese caso xa sabemos que non é posible, $A(2, n/5)$ é un múltiplo ondulante de $n/5$, entón $5 \cdot A(2, n/5)$ é un múltiplo ondulante de n.

Vexamos agora se $n = 2^{2\cdot r+1}$ ten un múltiplo ondulante. Primeiro vexamos que 8 é un múltiplo ondulante de 8, polo que sabemos que para $t = 1$, $2^{2\cdot t+1}$ ten un múltiplo ondulante de $2 \cdot t - 1$ cifras. Supoñamos que isto e certo para $t = k$ e vexamos que pasa para $t = k + 1$. Sexa A múltiplo ondulante de $2^{2\cdot k+1}$ con $2 \cdot k - 1$ cifras, polo tanto $B(k+1) = 10^{2\cdot k} \cdot b + A$ é un número ondulante para $b \in \{1, \dots, 9\}$ e $10^{2\cdot k} \cdot b + A = 10^{2\cdot k} \cdot b + 2^{2\cdot k+1} \cdot b' = 2^{2\cdot k} \cdot (5^{2\cdot k} \cdot b + 2 \cdot a)$. Polo tanto para que $B(k+1)$ sexa múltiplo de $2^{2\cdot k+3}$ tense que cumprir que $5^{2\cdot k} \cdot b + 2 \cdot a \equiv 0 \pmod{8}$ e como $5^2 \equiv 2 \pmod{8}$ temos que $2 \cdot b + 2 \cdot a \equiv 0 \pmod{8}$, entón $b + a \equiv 0 \pmod{4}$.

Por último obsérvese que os números da forma $2^{2\cdot k+1} \cdot m$ para r natural e m non é múltiplo de 5 o produto de $A(2 \cdot k + 1, m) \cdot B(k)$ é un múltiplo ondulante de $2^{2\cdot k+1} \cdot m$.

Problema 3.15 (IMO 1959 Problema 1). Proba que $\frac{21n+4}{14n+3}$ é irreducible para todo $n \in \mathbb{N}$. [5]

Solución Supoñamos que $\frac{21n+4}{14n+3}$ é reducible para algún $n \in \mathbb{N}$, entón $21n + 4 \equiv 0 \pmod{s}$ e $14n + 3 \equiv 0 \pmod{s}$ para algún $s \neq 1$ divisor común de $21n + 4$ e $14n + 3$. Polo tanto podemos dicir que $21n + 4 - (14n + 3) = 7n + 1 \equiv 0 \pmod{s}$ e por tanto $7n \equiv -1 \pmod{s}$.

Agora temos que $3 \cdot (7n - 1) \equiv 0 \pmod{s}$ é dicir $21n - 3 \equiv 0 \pmod{s}$ e como $21n - 4 \equiv 0 \pmod{s}$ e aplicando a propiedade transitiva, obtemos que: $21n - 4 \equiv 21n - 3 \pmod{s}$ se, e só se, $-4 \equiv -3 \pmod{s}$ se, e só se, $-1 \equiv 0$

(mód s). [3]

Problema 3.16 (IMO 1960 Problema 1). Determinar todo-los números de 3 díxitos N divisibles entre 11 e que $\frac{N}{11}$ é igual a suma dos cadrados dos díxitos de N. [5]

Solución Digamos que $N = abc = 100a + 10b + c$ e sabemos que $100a + 10b + c \equiv 0$ (mód 11). Como $10 \equiv -1 \pmod{11}$ aplicando el corolario 1.13 podemos dicir que $a - b + c \equiv 0 \pmod{11}$ e disto seguese que, ou $b = a + c$ ou $b = a + c - 11$ xa que $-9 \leq a - b + c \leq 18$.

- *Caso $b = a + c$:*
  $\frac{100a+10(a+c)+c}{11} = \frac{110a+11c}{11} = 10a + c = \frac{N}{11} = a^2 + (a + c)^2 + c^2 = 2a^2 + 2ac + 2c^2$, entón $2a^2 + (2c - 10)a + (2c^2 - c) = 0$, entón $a = \frac{10-2c\pm\sqrt{(2c-10)^2-4\cdot2\cdot(2c^2-c)}}{4} = \frac{10-2c\pm\sqrt{-12c^2-32c+100}}{4}$. Como $-12c^2 - 32c + 100$ só é positivo para $c = 0$ e $c = 1$ e para $c = 1$ $-12c^2 - 32c + 100 = 66$ con raíz irracional $c = 0$, entón $a = 0$ ou $a = 5$. Se $a = 0$, entón $b = 0$, polo que o número resultante será o 000 e se $a = 5$, entón $b = 5$, polo que o número resultante será o 550

- *Caso $b = a + c - 11$:*
  $\frac{100a+10(a+c-11)+c}{11} = \frac{110a+11c-110}{11} = 10a + c - 10 = \frac{N}{11} = a^2 + (a + c - 11)^2 + c^2 = 2a^2 + 2ac + 2c^2 - 22a - 22c$, entón $2a^2 + (2c - 32)a + (2c^2 - 23c + 131) = 0$, entón $a = \frac{32-2c\pm\sqrt{(2c-32)^2-4\cdot2\cdot(2c^2-23c+131)}}{4} = \frac{32-2c\pm\sqrt{-12c^2-56c-24}}{4}$.

  Como $-12c^2-56c-24$ só é positivo para $c = 1$, $c = 2$, $c = 3$ e $c = 4$. Para $c = 1$ $-12c^2 - 56c - 24 = 24$ con raíz irracional, para $c = 2$ $-12c^2 - 56c - 24 = 40$ con raíz irracional, para $c = 3$ $-12c^2 - 56c - 24 = 36$ con raíz 6 e para $c = 4$ $-12c^2 - 56c - 24 = 8$ con raíz irracional, entón $c = 3$, entón $a = 8$ o $a = 5$. Se $a = 8$, entón $b = 0$ resultando no número 803 e se $a = 5$, entón $b = -3$, polo que non é posíbel. [3]

Polo tanto as solucións ó problema salvo a trivial serán 550 e 803.

Problema 3.17 (IMO 1975 Problema 4). Cando 4444^{4444} escríbese en notación decimal dicimos que a suma dos seus díxitos é A. Sexa ademais B a suma dos díxitos de A. Calcula a suma dos díxitos de B. [5]

Demostración. Notemos primeiro que como $4444^{4444} < 10000^{4444} = 10^{17776}$, polo que 4444^{4444} ten como moito 17776 cifras de xeito que $A < 9 \cdot 17775 = 159975$, entón $B \leq 45$ e, polo tanto, a suma das cifras de B é como moito 12.

Ademais sabemos que $4444^{4444} \equiv A \equiv B \pmod 9$ ademais vexamos que $4444 \equiv 7 \pmod 9$, $4444^2 \equiv 4 \pmod 9$ e $4444^3 \equiv 1 \pmod 9$ e ademais $4444 = 3{\cdot}1481{+}1$, polo tanto $4444^{4444} \equiv 4444 \equiv 7 \pmod 9$, entón a suma dos díxitos de B da 7. [3] □

Problema 3.18 (IMO 1978 Problema 1978). Sexan m e n enteiros positivos tales que $1 \leq m < n$. Os últimos 3 díxitos de 1978^m coinciden cos últimos 3 díxitos de 1978^n nas súas representacións decimais. Encontra m e n tales que $m + n$ teñan valor mínimo. [5]

Problema 3.19 (IMO 1983 Problema 3). Sexan $a,\ b,\ c$ enteiros positivos coprimos dous a dous. Demostra que $2 \cdot a \cdot b \cdot c - a \cdot b - b \cdot c - c \cdot a$ é o maior enteiro que non pode ser expresado da forma $x \cdot b \cdot c + y \cdot c \cdot a + z \cdot a \cdot b$ sendo $a\ y\ z$ enteiros non negativos. [5]

Problema 3.20 (IMO 1986 Problema 1). Sexa d calquera enteiro positivo distinto de 2, 5 ou 13. Demostra que se pode encontrar $a, b \in \{2, 5, 13, d\}$ tal que $a \cdot b - 1$ non sexa un cadrado perfecto. [5]

Problema 3.21 (IMO 2000 Problema 5). Existe algún enteiro positivo n tal que teña exactamente 2000 divisores primos e divida a $2^n + 1$? [5]

Problema 3.22 (IMO 1964 problema 1). (a) Encontra todos os enteiros n para os cales $2^n - 1$ é divisible entre 7.

(b) Proba que non existe ningún enteiro positivo n para os cales $2^n + 1$ son divisibles entre 7. [5]

Solución

Os residuos asociados a 2^n son $\{2^1 \mod 7 = 2,\ 2^2 \mod 7 = 4,\ 2^3 \mod 7 = 1\}$, polo tanto cúmprese que $2^n - 1$ é un múltiplo de 7 sé e só se n é un múltiplo de 3.

Ademais como xa coñecemos os residuos de 2^n vexamos que ao sumarlles 1 ningún da un múltiplo de 7.

3.3. Outros problemas

Problema 3.23. Dado un número natural n, denotaremos $s(n)$ como a suma dos díxitos de n. Achar todas as solucións de la ecuación $n + s(n) + s(s(n)) = 2018$ [4]

Solución

Sabemos que $a \equiv s(a) \pmod 3$ para todo $a \in \mathbb{N}$, entón $n \equiv s(n) \pmod 3$, $s(n) \equiv s(s(n)) \pmod 3$, entón $n + s(n) + s(s(n)) \equiv s(n) + s(n) + s(n) = 3 \cdot s(n) \equiv 0 \pmod 3$, pero como $2018 \equiv 2 \pmod 3$ non existe ningún $n \in \mathbb{N}$ que sexa solución da ecuación.

Problema 3.24. Sexan $a,\ p,\ n \in \mathbb{N}$ enteiros positivos con p primo. Demostrar que se $2^p + 3^p = a^n$, entón $n = 1$. [4]

Solución

Para $p = 2$ temos que $2^2 + 3^2 = 13$, entón $n = 1$

No resto de casos vexamos que p é impar e, polo tanto, $2^p + 3^p \equiv 2^p + (-2)^p = 0 \pmod 5$, polo tanto $5 \mid 2^p + 3^p$.

Vexamos se 25 divide a $2^p + 3^p$, para iso observemos que $2^p + 3^p = 2^p + (5-2)^p = 2^p + \sum_i^p \binom{p}{i=0} \cdot 5^i \cdot (-2)^{p-i} = 2^p - 2^p + p \cdot 2^{p-1} \cdot 5 + \sum_i^p \binom{p}{i=2} \cdot 5^i \cdot (-2)^{p-i} \equiv 2^{p-1} \cdot 5 \pmod{25}$ que para $p \neq 5$ 25 non divide a $2^p + 3^p$, polo tanto $n = 1$. Se $p = 5$ teremos que $2^5 + 3^5 = 32 + 243 = 275 = 25 \cdot 11$, é dicir, $n = 1$.

Problema 3.25. Probar que entre 39 números naturais consecutivos, sempre existe un tal que la suma das súas cifras sexa múltiplo de 11. [4]

Solución

Sexan $a,\ a+1,\ a+2, \ldots, a+38$ os 39 números consecutivos sendo a da forma $a = a_n a_{n-1} \ldots a_2 a_1 a_0$ e definindo $s(a+i)$ a suma das cifras de a+i. Para $a_1 a_0 < 62$ a suma so variaría dependendo dos 2 últimas cifras e, en caso contrario, dependería das 3 últimas.

No caso de que $a_1 a_0 < 62$ supoñamos, sen perda de xeralidade, que $a_n + a_{n-1} + \ldots + a_3 + a_2 \equiv 0 \pmod{11}$ se $0 \leq i \leq 9$, entón $s(a+i) \mod 11 \in \{a_1 + a_0, \ldots a_1 + 9, a_1 + 1, \ldots a_1 + a_0\}$ dando 8 resultados distintos. Para $10 \leq i \leq 19$, $s(a+i) \mod 11 \in \{a_1 + a_0 + 1, \ldots a_1 + 10, a_1 + 2, \ldots a_1 + a_0 + 1\}$ engadindo unha suma distinta extra. Para $20 \leq i \leq 29$, $s(a+i) \mod 11 \in \{a_1 + a_0 + 2, \ldots a_1 + 11, a_1 + 3, \ldots a_1 + a_0 + 2\}$ dando outra suma distinta extra para un total de 11.

O argumento sería similar para $a_1 \in \{7, 8, 9\}$ facendo un argumento similar para cada un dos casos tendo en conta o cambio de decenas.

Problema 3.26. Demostrar que se n é impar entón $2^n + 3^n$ non é un cadrado perfecto. [4]

Solución

Tomando as congruencias módulo 3 temos que, para n enteiro impar $3^n \equiv 0 \pmod 3$ e $2^n \equiv 2 \pmod 3$, pero como $x^2 \equiv 0,\ 1 \pmod 3$ e como $2^n + 3^n \equiv 2 \pmod 2$ non pode ser un cadrado perfecto.

Problema 3.27. Supoñamos que un número primo escríbese como a suma dos cadrados perfectos de outros 3 números primos. Demostra que un dese primos ten que ser igual a 3. [4]

Solución

Supoñamos que $p = p_1^2 + p_2^2 + p_3^3$ sendo $p,\ p_1,\ p_2,\ p_3$ primos. En módulo 3 sabemos que se $p_i = 3$, entón $p_i^2 \equiv 0 \pmod 3$ ou $p_i^2 \equiv 1 \pmod 3$. Se p_i distinto de 0 temos que $p \equiv 1 + 1 + 1 = 3 \pmod 3$ entón $p = 3$ o cal é imposible xa que $p \geq 4 + 4 + 4 = 12$.

Problema 3.28. Demostrar que se $p \leq 7$ é un número primo e k é un número natural calquera, entón existe unha potencia de p cuxa representación decimal ten k ceros consecutivos. [4]

Solución

Vexamos se existe n natural tal que p^n acaba en 1 seguido de k ceros, ou o que é o mesmo $p^n \equiv 1 \pmod{10^{k+1}}$. Como $10^{k+1} = 2^{k+1} \cdot 5^{k+1}$ e $\varphi(10^{k+1}) = 2^k \cdot 4 \cdot 5^k$ e $(p, 10^{k+1}) = 1$ polo teorema de Euler podemos tomar $n = 2^k \cdot 4 \cdot 5^k$.

Problema 3.29. Escribimos os números de 1 ao vinte de xeito consecutivo formando o número de 31 cifras: $N = 1234567891011121314151617181920$.

Podemos reordear as cifras de N para obter un cadrado perfecto? [4]

Solución

Observese que $a^2 \mod 9 \in \{0,\ 1,\ 2,\ 4,\ 7\}$ e ademais a suma de todos os termos de N é $102 \equiv 3 \pmod 9$, polo tanto ningunha reordeación das cifras de N pode ser un cadrado perfecto.

Problema 3.30. Calcular o seguinte máximo común divisor: $((2^{2009}+1)^{2009}, 2^{2009^{2009}} + 1)$ [4]

Problema 3.31. Demostrar a veracidade ou falsedade das seguintes afirmacións:

- A suma dos cubos de tres enteiros consecutivos é un múltiplo de 9.
- A suma dos cubos de cinco enteiros consecutivos é un múltiplo de 25.

- A suma das potencias quintas de cinco enteiros consecutivos é un múltiplo de 25.

[4]

Problema 3.32. Dado un número primo $p \leq 7$ acha os posibles restos de dividir p^2 entre 30 [4]

Solución

Como p é impar temos que $p^2 \equiv 1 \pmod 2$, como p non é un múltiplo de 3, entón $p^2 \equiv 1 \pmod 3$.

De isto sabemos que $p^2 = 2 \cdot x + 1$ e $p^2 = 3 \cdot y + 1$ e, polo tanto, $2 \cdot x = 3 \cdot y$, polo que $x = 3 \cdot x'$, entón $p^2 = 6 \cdot x' + 1$ e, polo tanto, $p^2 \equiv 1 \pmod 6$.

Por outra banda $a^2 \mod 30 \in \{1,\ 7,\ 13,\ 19,\ 25\}$ para todo a natural, pero como $25 \nmid p^2$, entón $p^2 \mod 5 \in \{1,\ 4\}$ e, polo tanto, $p^2 \mod 30 \in \{1,\ 19\}$.

Bibliografía

[1] Durbin, John R., *Modern Algebra: An Introduction*, 6th ed., Wiley, New York, 2009.

[2] Gauss, C. F., *Disquisitiones Arithmeticae*, tradución ao ingles de Arthur A. Clarke S.J. Yale University Press, 1965.

[3] *https://artofproblemsolving.com/wiki/index.php/IMO_Problems_and_Solution* (Consultado o 29/07/2022)

[4] *http://wpd.ugr.es/ jmmanzano/preparacion/apuntes.php?id=4* (Consultado o 29/07/2022)

[5] *https://www.imo-official.org/problems.aspx* (Consultado o 29/07/2022)

[6] *http://www.olimpiadamatematica.es* (Consultado o 29/07/2022)

[7] *Olimpiada Matemática Española*, Real Sociedad Matemática Española, 2004.