ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

NGUYỄN THỊ HẰNG

CÁC BÀI TOÁN VỀ ĐỒNG DƯ VÀ HÀM SỐ HỌC

LUẬN VĂN THẠC SĨ KHOA HỌC

Hà Nội – 2015

ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

NGUYỄN THỊ HẰNG

CÁC BÀI TOÁN VỀ ĐỒNG DƯ VÀ HÀM SỐ HỌC

Chuyên ngành : PHƯƠNG PHÁP TOÁN SƠ CẤP

Mã số : 60 46 01 13

LUẬN VĂN THẠC SĨ KHOA HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS VŨ ĐỖ LONG

Hà Nội – 2015

MỤC LỤC

Lời mở đầu

Số học là một phần rất quan trọng của Toán học, ngay từ lúc bước vào bậc THCS học sinh đã được làm quen với các bài toán số học. Chính vì thế mà trong các đề thi Olympic, đề thi học sinh giỏi, các đề thi vào THPT chuyên khối khoa học tự nhiên ta đều thấy xuất hiện các bài toán số học. Mặc dù được làm quen sớm với số học nhưng khi gặp các bài toán dạng này học sinh vẫn thấy khó khăn trong cách giải quyết, đó là do khi học dần lên các lớp cao lượng kiến thức về số học lại giảm đi mà không được hệ thống hay nhắc lại thường xuyên. Chính vì vậy, em lựa chọn đề tài luận văn là " Các bài toán về đồng dư và hàm số học" nhằm hệ thống lại kiến thức và phân dạng các bài tập số học.

Trong luận văn em không đi sâu về trình bày lí thuyết mà chỉ hệ thống lại những kiến thức cơ bản để làm cơ sở giải quyết các dạng bài tập. Luận văn chủ yếu phân dạng và sắp xếp bài tập từ dễ tới khó trong đó có trình bày lời giải chi tiết giúp người đọc có thể tham khảo trong quá trình ôn tập kiến thức số học. Luận văn được chia thành ba chương:

Chương I trình bày các bài toán về số nguyên như các bài toán về phép chia hết, các bài toán liên quan đến số nguyên tố, ước chung lớn nhất, bội chung nhỏ nhất.

Chương II là phần trọng tâm của luận văn, trình bày các ứng dụng của lí thuyết đồng dư vào giải các bài toán chia hết, bài toán về số chính phương, chữ số tận cùng, các bài toán về phương trình nghiệm nguyên, phương trình đồng dư.

Chương III trình bày các bài toán về hàm số số học, trong đó các bài tập chủ yếu về hàm Euler $\varphi(n)$, hàm tổng các ước $\sigma(n)$, hàm số các ước số $\tau(n)$ của một số tự nhiên.

Do thời gian và kiến thức còn hạn chế nên trong quá trình viết luận văn, giải quyết các bài tập chắc chắn không tránh khỏi những thiếu xót. Em rấy mong nhận được sự góp ý của các thầy cô và các bạn để luận văn được hoàn thiện hơn.

Trong quá trình làm luận văn, em đã được thầy PGS. TS Vũ Đỗ Long – Trường Đại học Khoa học tự nhiên – Đại học Quốc gia Hà Nội hướng dẫn, chỉ bảo tận tình. Nhân dịp này em xin bày tỏ lòng biết ơn sâu sắc tới thầy. Em xin chân thành cảm ơn các thầy cô trong tường Đại học Khoa học tự nhiên – Đại học Quốc

gia Hà Nội đã dạy dỗ, trang bị kiến thức bổ ích và giúp đỡ em trong suốt quá trình theo học. Em cũng xin chân thành cảm ơn ban chủ nhiệm khoa Toán – Cơ – Tin học đã giúp đỡ, tạo điều kiện cho em trong quá trình hoàn thiện luận văn.

Hà Nội, tháng 5 năm 2015

Tác giả luận văn

Nguyễn Thị Hằng

Chương 1. Số nguyên và tính chia hết

1.1. Kiến thức cơ bản

1.1.1. Phép chia trong ℤ

Chúng ta nói rằng số nguyên a chia hết cho số nguyên b ≠ 0, hay a là bội của b, kí hiệu a ⋮ b, nếu có số nguyên c để a = bc. Trong trường hợp này ta cũng nói là b chia hết a, hay b là ước (thừa số) của a, kí hiệu b | a. Ngược lại ta nói rằng a không chia hết cho b, hay b không chia hết a.

Ví dụ : 7 | 14 ; -8 | 24 ; 5 | -30 ; 15 | 0 ; 2 không chia hết 5 ; 6 không chia hết -13.

Định lí 1.1.1. Giả sử a, b là các số nguyên. Khi đó :

1. Nếu b | a và a > 0, b > 0 thì $1 \leq b \leq a$.

2. Nếu b | a và c | b thì c | a.

3. Nếu b | a và c ≠ 0 thì bc | ac.

4. Nếu c | a và c | b thì c | (ma + nb) với các số nguyên m, n bất kì.

Định lí 1.1.2. Giả sử a, b là các số nguyên, b ≠ 0. Khi đó tồn tại duy nhất các số nguyên q, r thỏa mãn : a = bq + r và $0 \leq r < |b|$.

Khi a = bq + r, $0 \leq r < |b|$ ta nói q là thương và r là phần dư trong phép chia a cho b. Hiển nhiên b | a khi r = 0.

Định lí 1.1.3. Nếu các số $a_1, a_2, \ldots, a_n$ chia hết cho m thì $a_1 + a_2 + \ldots + a_n$ chia hết cho m.

Hệ quả 1.1.1. Nếu tổng một số số hạng chia hết cho m và trừ một số hạng, còn tất cả các số khác đều chia hết cho m thì số hạng này cũng chia hết cho m.

Định lí 1.1.4. Nếu mỗi số a_i chia hết cho m_i ($1 \leq i \leq n$) thì tích $a_1a_2\ldots a_n$ đều chia hết cho tích $m_1m_2\ldots m_n$.

Hệ quả 1.1.2. Nếu a chia hết cho m thì với số tự nhiên n tùy ý a^n chia hết cho m^n.

Hệ quả 1.1.3. Nếu chỉ một thừa số chia hết cho m thì tích cũng chia hết cho m.

Định lí 1.1.5. Với mọi cặp số nguyên a, b mà a + b khác 0 và với mọi số nguyên không âm n tổng $a^{2n+1} + b^{2n+1}$ chia hết cho a + b.

Hệ quả 1.1.4. Với mọi cặp số nguyên a, b và với mọi số tự nhiên n đều có:

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

Định lí 1.1.6. Với mọi cặp số nguyên a, b mà a – b khác 0 và với mọi số tự nhiên n, số $a^n - b^n$ chia hết cho a – b

Hệ quả 1.1.5. Với mọi cặp số nguyên a, b mà $a^2 - b^2$ khác 0 và với mọi số nguyên dương n, số $a^{2n} - b^{2n}$ chia hết cho a + b

1.1.2. Số nguyên tố

Định nghĩa: Số tự nhiên p > 1 được gọi là số nguyên tố, nếu ngoài 1 và p nó không còn ước tự nhiên nào khác.

Số tự nhiên lớn hơn 1 có nhiều hơn 2 ước tự nhiên được gọi là hợp số.

Số 1 chỉ có đúng một ước số tự nhiên. Số 1 không phải là số tự nhiên cũng không phải là hợp số.

Bổ đề. Mọi số tự nhiên lớn hơn 1 đều có ít nhất một ước là số nguyên tố

Định lí 1.1.7. Nếu số tự nhiên a lớn hơn 1 và không chia hết cho các số nguyên tố bé hơn hoặc bằng $\sqrt{a}$ thì a là số nguyên tố.

Chứng minh: Giả sử a là hợp số, đặt a = mn, với m ≤ n. Khi đó a chia hết cho m và m ≤ $\sqrt{a}$

Giả sử m có ước nguyên tố là p thì p ≤ m. Suy ra a chia hết p và p ≤ $\sqrt{a}$, điều này trái với giả thiết a không chia hết cho các số nguyên tố bé hơn hoặc bằng $\sqrt{a}$.

Vậy a là số nguyên tố.

1.1.3. Ước chung lớn nhất và bội chung nhỏ nhất.

Nếu a, b là các số nguyên không đồng thời bằng không, thì tập các ước chung của a và b là hữu hạn và chứa các số +1 và -1. Chúng ta sẽ quan tâm đến số nguyên lớn nhất nằm trong các ước chung này.

Ước chung lớn nhất của hai số nguyên không đồng thời bằng không a và b là số nguyên lớn nhất chia hết đồng thời cả a và b.

Ước chung lớn nhất của hai số nguyên a và b được kí hiệu là (a, b).

Khái niệm ước chung lớn nhất của các số nguyên không đồng thời bằng không $a_1, a_2, ..., a_n$ được hiểu hoàn toàn tương tự như khái niệm ước chung lớn nhất của các số nguyên. Đó chính là số nguyên lớn nhất chia hết đồng thời tất cả các

$a_j, 1 \leq j \leq n$. Ước chung lớn nhất của các số nguyên $a_1, a_2, ..., a_n$ được kí hiệu là $(a_1, a_2, ..., a_n)$.

Chúng ta cũng quan tâm đến các cặp số nguyên mà chúng không có ước chung hơn 1. Các cặp số nguyên như vậy được gọi là nguyên tố cùng nhau.

Hiển nhiên là (a, b) = (b, a) và (a, b) = (|a|, |b|).

Định lí 1.1.8. Nếu a, b, c là các số nguyên và (a, b) = d thì :

1. $(\frac{a}{d}, \frac{b}{d}) = 1$

2. (a + cb, b) = (a, b)

Nếu a, b là các số nguyên, ta nói số nguyên dạng ma + nb là tổ hợp tuyến tính của a và b, trong đó m, n là các số nguyên.

Một tập $M \neq \Phi$ các số nguyên được gọi là một modulo nếu nó có tính chất: nếu m, n ∈ M thì m – n ∈ M.

Từ định nghĩa của modulo suy ra rằng, nếu m, n ∈ M, thì

0 = m – m ∈ M, - n = 0 – n ∈ M, m + n = m – (- n) ∈ M.

Nói một cách khác, nếu a, b ∈ M thì các tổ hợp tuyến tính của a và b cũng thuộc M. Modulo M = {0} được gọi là modulo tầm thường.

Định lí 1.1.9. Mỗi modulo không tầm thường M chính là tập tất cả các bội của một số nguyên dương nào đó.

Định lí 1.1.10. Giả sử a, b là các số nguyên không đồng thời bằng 0 và d = (a, b). Khi đó modulo M = {ax + by : x, y ∈ ℤ} chính là tập tất cả các bội của d.

Hệ quả 1.1.6 Giả sử d = (a, b) là ước chung lớn nhất của hai số nguyên a và b. Khi đó:

1. d là số nguyên dương nhỏ nhất là tổ hợp tuyến tính của a và b.

2. Mỗi ước chung của a và b đều là ước của d.

Định lí 1.1.11. Nếu $a_1, a_2, \ldots, a_n, a_{n+1}$ là các số nguyên khác không, n ≥ 2, thì

$(a_1, a_2, \ldots, a_n, a_{n+1}) = (a_1, a_2, \ldots, a_{n-1}, (a_n, a_{n+1}))$.

**) Thuật toán Euclid*

Định lí 1.1.12. Giả sử $r_0 = a$ và $r_1 = b$ là các số nguyên với $a \geq b > 0$. Nếu thuật toán chia được thực hiện liên tiếp $r_j = r_{j+1}q_{j+1} + r_{j+2}, 0 < r_{j+2} < r_{j+1}$ với j = 0, 1, 2, …, n – 2 và $r_{n+1} = 0$, thì $(a, b) = r_n$, là số dư khác không cuối cùng.

Chứng minh: Từ định lí 1.1.8 ta có nhận xét là: nếu c = dq + r thì

$$(c, d) = (c – qd, d) = (r, d) = (d, r).$$

Với $a = r_0$, $b = r_1$ tồn tại hai số nguyên q_1, r_2, sao cho:

$r_0 = r_1q_1 + r_2$ $\quad 0 < r_2 < r_1$

tồn tại q_2, r_3 sao cho:

$r_1 = r_2q_2 + r_3$ $\quad 0 < r_3 < r_2$

…

$r_{j-2} = r_{j-1}q_{j-1} + r_j$ $\quad 0 < r_j < r_{j-1}$

…

$r_{n-2} = r_{n-1}q_{n-1} + r_n$ $\quad 0 < r_n < r_{n-1}$

$r_{n-1} = r_nq_n + 0$

Từ nhận xét trên, ta có:

$(a, b) = (r_0, r_1) = (r_1, r_2) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, r_{n+1}) = (r_n, 0) = r_n$.

Quá trình trên gọi là thuật toán Euclid tìm ước chung lớn nhất của hai số a, b.

Định lí 1.1.13. Định lí cơ bản của số học:

Mọi số nguyên lớn hơn 1 đều viết được một cách duy nhất thành tích của các thừa số nguyên tố theo thứ tự không giảm.

Bổ đề 1.1.13.a. Nếu a, b, c là các số nguyên dương sao cho (a, b) = 1 và a | bc thì a | c.

Bổ đề 1.1.13.b. Nếu p là ước nguyên tố của tích $a_1, a_2, \ldots, a_k$, ở đây $a_1, a_2, \ldots, a_k$ là các số nguyên, thì có i, $1 \leq i \leq k$ để $p \mid a_i$.

Chứng minh định lí 1.1.13: Trước hết ta chứng minh bằng quy nạp theo n rằng mọi số nguyên lớn hơn 1 đều viết được thành tích của các thừa số nguyên tố. Trường hợp n = 2 là tầm thường. Số nguyên n + 1 > 2 nếu là số nguyên tố thì không có gì phải chứng minh. Ngược lại, ta có n + 1 = ab, với a > 1, b < n + 1; theo giả thiết quy nạp thì a, b đều là tích của các số nguyên tố.

Bây giờ ta chứng minh tính duy nhất của biểu diễn.

Giả sử $n = p_1p_2\ldots p_r = q_1q_2\ldots q_s$; với $p_1 \le p_2 \le \ldots \le p_r$, $q_1 \le q_2 \le \ldots \le q_s$ là các số nguyên tố.

Từ bổ đề 1.1.13.b suy ra r = s và $p_1 = q_1, \ldots, p_r = q_s$. ■

Chú ý:

1. Mọi số nguyên n > 1 đều có biểu diễn duy nhất

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \text{ , với } 1 \le k,\ 0 < \alpha_1, \ldots, \alpha_k.$$

2. Nếu dãy tất cả số nguyên tố được sắp theo thứ tự tăng dần :

$p_1 = 2 < p_2 = 3 < p_3 = 5 < p_4 = 7 < p_5 = 11 < \ldots$

thì mọi số nguyên dương đều được viết duy nhất dưới dạng

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \ldots$

trong đó $\alpha_k \ge 0$ và bằng 0 với hầu hết, trừ một số hữu hạn các giá trị của k.

Bội chung nhỏ nhất của hai số nguyên $a \ne 0$ và $b \ne 0$, kí hiệu là [a, b], được hiểu là số nguyên dương nhỏ nhất chia hết cho cả a và b.

Dễ dàng thấy rằng [a, b] = [b, a] và [a, b] = [|a|, |b|].

Bội chung nhỏ nhất của các số nguyên khác không $a_1, a_2, \ldots, a_k$, kí hiệu $[a_1, a_2, \ldots, a_k]$, là số nguyên dương nhỏ nhất chia hết tất cả các số a_j, $1 \le j \le k$.

Định lí 1.1.14. Nếu các số a, b có sự phân tích ra thừa số nguyên tố

$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ và $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$

thì
$$(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \ldots p_k^{\min\{\alpha_k,\beta_k\}},$$
$$[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \ldots p_k^{\max\{\alpha_k,\beta_k\}}$$

và (a, b). [a, b] = ab.

Chứng minh. Dễ dàng thấy rằng

$$c = \prod_{k=0}^{+\infty} p_k^{\gamma_k} \text{ là ước của } d = \prod_{k=0}^{+\infty} p_k^{\theta_k} \text{ khi và chỉ khi với mọi k: } \gamma_k \le \theta_k.$$

Từ đây dễ dàng suy ra

$$(a, b) = \prod_{k=0}^{+\infty} p_k^{\min\{\alpha_k,\beta_k\}} \quad , \quad [a, b] = \prod_{k=0}^{+\infty} p_k^{\max\{\alpha_k,\beta_k\}}$$

Ta có $\min\{\alpha_i,\beta_i\} + \max\{\alpha_i,\beta_i\} = \alpha_i + \beta_i$ nên

$$(a,b).[a,b] = \prod_{k=0}^{+\infty} p_k^{\min\{\alpha_k,\beta_k\}+\max\{\alpha_k,\beta_k} = \prod_{k=0}^{+\infty} p_k^{\alpha_k+\beta_k} = ab.$$

1.2. Bài toán chia hết.

Bài 1.1. Chứng minh rằng số $\underbrace{11\ldots11}_{81\text{ số }1}$ chia hết cho 81.

Lời giải:

Ta có: $\underbrace{11\ldots11}_{9\text{ số }1}$ chia hết cho 9 và $\underbrace{11\ldots11}_{81\text{ số }1} = \underbrace{11\ldots11}_{9\text{ số }1}(10^{72} + 10^{63} + \ldots + 10^9 + 1)$

Mà $10^{72} + 10^{63} + \ldots + 10^9 + 1$ có tổng các chữ số bằng 9 nên chia hết cho 9

Do đó số $\underbrace{11\ldots11}_{81\text{ số }1}$ chia hết cho 81.

Bài 1.2. Chứng minh rằng $\underbrace{\overline{aa\ldots a}}_{3^n\text{ chữ a}}$ chia hết cho 3^n, n > 0 (*)

Lời giải:

Ta chứng minh bài toán bằng quy nạp

Với n = 1, ta có $\overline{aaa}$ = 111a ⋮ 3. Vậy (*) đúng

Giả sử (*) đúng với n = k, tức là $\underbrace{\overline{aa\ldots a}}_{3^k\text{ chữ a}}$ chia hết cho 3^k

Ta cần chứng minh (*) cũng đúng với n = k + 1, nghĩa là $\underbrace{\overline{aa\ldots a}}_{3^{k+1}\text{ chữ a}}$ chia hết cho 3^{k+1}

Thật vậy, ta có $3^{k+1} = 3.3^k = 3^k + 3^k + 3^k$, nên

$$\underbrace{\overline{aa\ldots a}}_{3^{k+1}\text{ chữ a}} = \underbrace{\overline{aa\ldots a}}_{3^k\text{ chữ a}}\underbrace{\overline{aa\ldots a}}_{3^k\text{ chữ a}}\underbrace{\overline{aa\ldots a}}_{3^k\text{ chữ a}} = \underbrace{\overline{aa\ldots a}}_{3^k\text{ chữ a}}.10^{2.3^k} + \underbrace{\overline{aa\ldots a}}_{3^k\text{ chữ a}}.10^{3^k} + \underbrace{\overline{aa\ldots a}}_{3^k\text{ chữ a}} =$$

$$= \underbrace{\overline{aa\ldots a}}_{3^k\text{ chữ a}}(10^{2.3^k} + 10^{3^k} + 1) \vdots 3^k.3 = 3^{k+1}.$$

Vậy $\underbrace{\overline{aa\ldots a}}_{3^n\text{ chữ a}}$ chia hết cho 3^n, với n > 0.

Bài 1.3. Chứng minh rằng tồn tại một số tự nhiên gồm toàn chữ số 6 chia hết cho 2015.

Lời giải:

Xét các số 6, 66, 666, …, $\underbrace{66...6}_{2015 \text{ số } 6}$

Nếu có 1 trong 2015 số trên chia hết cho 2015 thì chứng minh xong

Nếu cả 2015 số trên không có số nào chia hết cho 2015 thì khi chia các số đó cho 2015 ta nhận được 2015 số dư nên có ít nhất 2 số có cùng số dư khi chia cho 2015. Giả sử 2 số đó là A = $\underbrace{66...66}_{\text{n số } 6}$, B = $\underbrace{66...66}_{\text{m số } 6}$ (m > n > 0).

Lấy A – B = $\underbrace{66...66}_{\text{m−n số } 6}\underbrace{00...0}_{\text{n số } 0}$ chia hết cho 2015. Do đó số $\underbrace{66...66}_{\text{m−n số } 6}$ chia hết cho 2015

Bài 1.4. Chứng minh rằng:

a. $A = 3 + 3^2 + 3^3 + … + 3^{100}$ chia hết cho 13

b. $B = 7 + 7^2 + 7^3 + … + 7^{60}$ chia hết cho 400

Lời giải:

a. $A = 3 + 3^2 + 3^3 + … + 3^{100}$

$= 3(1 + 3 + 3^2) + 3^4(1 + 3 + 3^2) + … + 3^{98}(1 + 3 + 3^2)$

$= 13.3 + 13.3^4 + … + 13.3^{98} = 13(3 + 3^4 + … + 3^{98})$ chia hết cho 13

b. $B = 7 + 7^2 + 7^3 + … + 7^{60}$

$= 7(1 + 7 + 7^2 + 7^3) + 7^5(1 + 7 + 7^2 + 7^3) + … + 7^{57}(1 + 7 + 7^2 + 7^3)$

$= 7.400 + 7^5.400 + … + 7^{75}.400 = 400(7 + 7^5 + … + 7^{57})$ chia hết cho 400.

Bài 1.5. Chứng minh rằng nếu số tự nhiên $\overline{abc}$ chia hết cho 37 thì các số $\overline{bca}$ và $\overline{cab}$ cũng chia hết cho 37.

Lời giải:

Ta có $\overline{abc} + \overline{bca} + \overline{cab} = 111(a + b + c) = 37.3(a + b + c)$ (1)

Vì $\overline{abc}$ chia hết cho 37 nên $100a + 10b + c = 37k$ ($k \in \mathbb{N}$).

$\overline{bca} = 100b + 10c + a = 10(100a + 10b + c) – 999a = 370k – 37.27a$ chia hết cho 37 (2)

Từ (1) và (2) suy ra $\overline{cab}$ chia hết cho 37.

Bài 1.6. Chứng minh rằng nếu các số nguyên x ,y mà $x^4 + y^4$ chia hết cho 5 thì x và y chia hết cho 5.

Lời giải:

Xét số dư khi chia x^4 cho 5 :

$x = 5k$ thì $x^2 = 25k^2$

$x = 5k \pm 1$ thì $x^2 = 25k^2 \pm 10k + 1$

$x = 5k \pm 2$ thì $x^2 = 25k^2 \pm 20k + 4 = 25k^2 \pm 20k + 5 - 1$

x^2 chia 5 có số dư là 0, 1, -1 nên x^4 chia 5 có số dư là 0, 1. Tương tự y^4 chia cho 5 cũng có số dư là 0, 1. Mà $x^4 + y^4$ chia hết cho 5 khi tổng số dư của x^4 và y^4 bằng 0. Điều này chỉ xảy ra khi x^4 chia hết cho 5, y^4 chia hết cho 5 hay x và y đều chia hết cho 5.

Bài 1.7. Chứng minh rằng: $A(n) = n(n^2 + 1)(n^2 + 4)$ chia hết cho 5 với mọi số tự nhiên n.

Lời giải:

Chia n cho 5 ta được các số dư là 0, ± 1, ± 2.

Khi đó :

Nếu $n = 5k$ (n chia hết cho 5) thì A(n) chia hết cho 5 do A(n) chứa một thừa số chia hết cho 5

Nếu $n = 5k \pm 1$ thì có $n^2 + 4 = 25k^2 \pm 10k + 5 = 5(5k^2 \pm 2k + 1)$ chia hết cho 5 nên A(n) chia hết cho 5 .

Nếu $n = 5k \pm 2$ thì có $n^2 + 1 = 25k^2 \pm 10k + 5 = 5(5k^2 \pm 2k + 1)$ chia hết cho 5 nên A(n) chia hết cho 5.

Trong mọi trường của số dư khi chia n cho 5, A(n) đều chia hết cho 5 nên A(n) chia hết cho 5 với mọi n.

Bài 1.8. Tìm số tự nhiên n để $2^n - 1$ chia hết cho 7.

Lời giải:

Biểu diễn n dưới dạng $n = 3k + r$, $r \in \{0; 1; 2\}$, $k \in \mathbb{N}$

Nếu $r = 0$ thì $n = 3k$ và $2^n - 1 = 2^{3k} - 1 = 8^k - 1 = (8 - 1)(8^{k-1} + 8^{k-2} + \ldots + 1)$

Nếu $r = 1$ thì $n = 3k + 1$ và $2^n - 1 = 2^{3k+1} - 1 = 2.2^{3k} - 1 = 2(2^{3k} - 1) + 1$.

Mà $2^{3k} - 1 \vdots 7$ nên $2^n - 1$ chia 7 dư 1.

Nếu $r = 2$ thì $n = 3k + 2$ và $2^n - 1 = 2^{3k+2} - 1 = 4.2^{3k} - 1 = 4(2^{3k} - 1) + 3$.

Mà $2^{3k} - 1 \vdots 7$ nên $2^n - 1$ chia 7 dư 3.

Vậy n = 3k thì $2^n - 1$ chia hết cho 7.

Bài 1.9. Chứng minh rằng: $x^{3k+2} + x^{3t+1} + 1$ chia hết cho $x^2 + x + 1$, với k, t là số tự nhiên.

Lời giải:

+) Nếu $k \geq t$, khi đó: $x^{3k+2} + x^{3t+1} + 1 = (x^{3k+2} - x^{3t+2}) + (x^{3t+2} + x^{3t+1} + x^{3t}) - (x^{3t} + 1)$

Thấy $x^{3k+2} - x^{3t+2} = x^{3t+2}(x^{3k-3t} - 1) = x^{3t+2}[(x^{k-t})^3 - 1] \vdots [(x^{k-t})^3 - 1] \vdots x^3 - 1 \vdots x^2 + x + 1$

$x^{3t+2} + x^{3t+1} + x^{3t} = x^{3t}(x^2 + x + 1) \vdots x^2 + x + 1$

$x^{3t} + 1 \vdots x^3 - 1 \vdots x^2 + x + 1.$

Do đó $x^{3k+2} + x^{3t+1} + 1$ chia hết cho $x^2 + x + 1$

+) Nếu $t \geq k$, làm tương tự trường hợp trên ta có điều phải chứng minh.

Bài 1.10. Cho 3 số nguyên dương a, b, c thỏa mãn $a^2 = b^2 + c^2$. Chứng minh rằng M = abc chia hết cho 60.

Lời giải:

Có 60 = 3.4.5 và 3, 4, 5 đôi một nguyên tố cùng nhau

+) Nếu a, b, c đều không chia hết cho 3 thì a^2, b^2, c^2 chia cho 3 đều có số dư là 1. Khi đó $a^2 \neq b^2 + c^2$, do đó phải có ít nhất một trong 3 số chia hết cho 3. Vậy M chia hết cho 3 (1)

+) Nếu a, b, c đều không chia hết cho 5 thì a^2, b^2, c^2 chia cho 5 đều có số dư là 1 hoặc 4. Khi đó $b^2 + c^2$ chia 5 dư 0, 2 hoặc 3, do đó $a^2 \neq b^2 + c^2$. Vậy phải có ít nhất 1 số chia hết cho 5 hay M chia hết cho 5 (2)

+) Nếu a, b, c là các số lẻ thì a^2, b^2 và c^2 chia cho 4 đều dư 1. Khi đó $b^2 + c^2$ chia 4 dư 2, do đó $a^2 \neq b^2 + c^2$. Vậy ít nhất 1 trong 2 số b hoặc c phải chẵn.

Giả sử b chẵn:

Nếu c chẵn thì M chia hết cho 4.

Nếu c lẻ, mà $a^2 = b^2 + c^2$ nên a lẻ. Khi đó $b^2 = (a - c)(a + c)$ suy ra $(\frac{b}{2})^2 = (\frac{a-c}{2})(\frac{a+c}{2})$, từ đây ta được $\frac{b}{2}$ là số chẵn và b chia hết cho 4. Vậy M chia hết cho 4 (3)

Từ (1), (2), (3) suy ra M chia hết cho 60.

Bài 1.11. Chứng minh rằng: từ $2^{n+1} - 1$ số nguyên bất kì luôn tìm được 2^n số mà tổng của chúng chia hết cho 2^n, với n là số tự nhiên (*). *(Trích tài liệu [5])*

Lời giải:

Với n = 1, ta thấy trong 3 số tự nhiên bất kì luôn có ít nhất 2 số có cùng tính chẵn lẻ nên tổng của 2 số này chia hết cho 2. Vậy (*) đúng với n = 1.

Giả sử (*) đúng với n = k, tức là từ $2^{k+1} - 1$ số nguyên bất kì luôn tìm được 2^k số mà tổng của chúng chia hết cho 2^k.

Ta cần chứng minh (*) cũng đúng với n = k + 1, nghĩa là: từ $2^{k+2} - 1$ số nguyên bất kì luôn tìm được 2^{k+1} số mà tổng của chúng chia hết cho 2^{k+1}

Thật vậy, ta có $2^{k+2} - 1 = 2.2^{k+1} - 1 = 2(2^{k+1} - 1) + 1$

Theo giả thiết quy nạp, từ $2^{k+1} - 1$ số nguyên bất kì luôn tìm được 2^k số mà tổng của chúng chia hết cho 2^k, gọi tổng đó là $S_1 = 2^k q_1$ ($q_1 \in \mathbb{Z}$).

Trong $2^{k+1} - 1$ số khác với $2^{k+1} - 1$ số ở trên cũng có 2^k số có tổng chia hết cho 2^k, gọi tổng đó là $S_2 = 2^k q_2$ ($q_2 \in \mathbb{Z}$).

Như vậy, ta có $2^k + 2^k = 2^{k+1}$ số có tổng $S_1 + S_2 = 2^k(q_1 + q_2)$. Còn lại $2^{k+2} - 1 - 2^{k+1} = 2^{k+1} - 1$ số. Theo giả thiết quy nạp thì trong $2^{k+1} - 1$ số này cũng có 2^k số có tổng chia hết cho 2^k, gọi tổng này là $S_3 = 2^k q_3$ ($q_3 \in \mathbb{Z}$).

Do đó, ta có $S_1 + S_2 + S_3 = 2^k(q_1 + q_2 + q_3)$ chia hết cho 2^k. Mà trong 3 số nguyên q_1, q_2, q_3 có 2 số có tổng chia hết cho 2, giải sử là $q_1 + q_2$ chia hết cho 2. Khi đó tổng của 2^{k+1} số là $S_1 + S_2 = 2^k(q_1 + q_2)$ chia hết cho $2.2^k = 2^{k+1}$. Chính vì thế (*) đúng với n = k + 1.

Vậy, từ $2^{n+1} - 1$ số nguyên bất kì luôn tìm được 2^n số mà tổng của chúng chia hết cho 2^n, với n là số tự nhiên.

Bài 1.12. Cho 2015 số tự nhiên bất kì. Chứng minh rằng trong các số đó có một số chia hết cho 2015 hoặc có một số số có tổng chia hết cho 2015.

Lời giải:

Gọi 2015 số đó là $a_1, a_2, \ldots, a_{2015}$.

Đặt $s_1 = a_1$

$s_2 = a_1 + a_2$

$s_3 = a_1 + a_2 + a_3$

.

.

.

$s_{2015} = a_1 + a_2 + \ldots + a_{2015}$

Chia tất cả các số hạng của dãy trên cho 2015.

Nếu có một số hạng của dãy chia hết cho 2015 thì bài toán đã được chứng minh.

Nếu không có số hạng nào của dãy chia hết cho 2015 thì ta thấy có tất cả 2015 phép chia mà số dư tối đa chỉ gồm 2014 giá trị có thể là 1, 2, 3, …, 2014. Do đó có ít nhất hai số hạng của dãy có cùng số dư khi chia cho 2015. Giả sử hai số đó là :

$s_i = a_1 + a_2 + \ldots + a_i$

$s_j = a_1 + a_2 + \ldots + a_j$

với i, j là hai số tự nhiên, $1 \leq i \leq j \leq 2015$. Khi đó $s_j - s_i$ chia hết cho 2015

Chính vì thế $a_{i+1} + a_{i+2} + \ldots + a_j$ chia hết cho 2015.

Vậy trong 2015 số tự nhiên bất kì có một số chia hết cho 2015 hoặc có một số số có tổng chia hết cho 2015.

Bài 1.13. Chứng minh rằng (a + b)! chia hết cho a!b! với mọi số tự nhiên a, b.

Lời giải:

Nếu ít nhất 1 trong 2 số a hoặc b bằng 1, giả sử a = 1, với mọi số tự nhiên b ta có: (b + 1)! = b!(b + 1). Do đó (b + 1)! chia hết cho 1!b!. Vậy biểu thức đúng với $a + b \leq 3$.

Giả sử n là số tự nhiên lớn hơn 2 và biểu thức đúng với mọi cặp số a, b có tổng a + b không vượt quá n. Ta sẽ chứng minh biểu thức cũng đúng với cặp số a, b có a + b = n + 1.

Thật vậy, ta có:

(a - 1) + b = n thì (a + b - 1)! chia hết cho (a - 1)!b!, mà (a - 1)!a = a! nên

(a + b - 1)!a chia hết cho a!b!

a + (b - 1) = n thì (a + b - 1)! chia hết cho a!(b - 1)!, mà (b - 1)!b = b! nên

(a + b - 1)!b chia hết cho a!b!

Cộng lại ta có (a + b - 1)!a + (a + b - 1)!b chia hết cho a !b!

hay (a + b - 1)!(a + b) chia hết cho a!b! hay (a + b)! chia hết cho a!b!. Do đó biểu thức đúng với mọi cặp số tự nhiên có tổng a + b = n + 1.

Vậy (a + b)! chia hết cho a!b! với mọi số tự nhiên a, b.

Bài 1.14. Tìm tất cả các số tự nhiên n sao cho (n - 1)! chia hết cho n.

Lời giải:

Ta có (n - 1)! = 1.2.3…(n - 1)

+) Nếu n là số nguyên tố thì (n - 1)! không chia hết cho n.

+) Nếu n là hợp số có dạng n = ab với a khác b và $1 < a < n$, $1 < b < n$ thì trong tích 1.2.3…(n - 1) có 2 thừa số a, b nên (n - 1)! chia hết cho n

+) Nếu n là hợp số có dạng $n = p^2$, với p là số nguyên tố:

Nếu p = 2 thì n = 4 không là ước của 3!

Nếu p > 2 thì $p^2 - 1 \geq 2p$, do đó $2p^2 = p.2p$ là ước của (n - 1)! nên $p^2 = n$ là ước của (n – 1)!

Vậy (n - 1)! chia hết cho n khi n là hợp số và n khác 4.

Bài 1.15. Cho x, y là hai số nguyên khác (-1) sao cho $\frac{x^3+1}{y+1}+\frac{y^3+1}{x+1}$ là số nguyên. Chứng minh rằng $x^{2016} - 1 \vdots y + 1$.

Lời giải :

Đặt $\frac{x^3+1}{y+1}=\frac{a}{b},\frac{y^3+1}{x+1}=\frac{c}{d}$, a, b, c, d là các số nguyên tố và

b > 0, d > 0, (a, b) = 1, (c, d) = 1. Ta có $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \in \mathbb{Z}$ nên $ad + bc \vdots bd$, suy ra $ad \vdots b$, vì (a, b) = 1 nên $d \vdots b$ (1).

Mặt khác, $\frac{a}{b}.\frac{c}{d}=\frac{x^3+1}{y+1}.\frac{y^3+1}{x+1} = (x^2 - x + 1)(y^2 - y + 1) \in \mathbb{Z}$ nên $ac \vdots bd$, suy ra $ac \vdots d$, vì (c, d) = 1 nên $a \vdots d$ (2).

Từ (1) và (2), ta được $a \vdots b$, mà (a, b) = 1 nên b = 1.

Vì $\frac{a}{b}=\frac{x^3+1}{y+1} \Leftrightarrow x^3 + 1 = a(y + 1)$ nên $x^3 + 1 \vdots y + 1$ (3)

Mà $x^{2016} - 1 = (x^3)^{672} - 1 \vdots x^3 - 1$, kết hợp với (3), ta được $x^{2016} - 1 \vdots y + 1$.

Bài 1.16. Cho f(x) là đa thức với hệ số nguyên

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ $(a_i \in \mathbb{Z}, i = 1, 2, \ldots, n)$

1. Cho a, b là hai số nguyên khác nhau, chứng minh rằng f(a) – f(b) chia hết cho a – b.

2. Cho c, d là hai số nguyên tố cùng nhau, chứng minh rằng f(c + d) chia hết cho cd khi và chỉ khi f(c) chia hết cho d và f(d) chia hết cho c.

(Trích tài liệu [5])

Lời giải:

1. Ta có $f(a) = a_n a^n + a_{n-1}a^{n-1} + \ldots + a_1 a + a_0$

$f(b) = a_n b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0$

Khi đó $f(a) - f(b) = a_n(a^n - b^n) + a_{n-1}(a^{n-1} - b^{n-1}) + \ldots + a_1(a - b)$

$= (a - b)[a_n(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}) + a_{n-1}(a^{n-2} + a^{n-3}b + \ldots + b^{n-2}) + \ldots + a_1]$ chia hết cho a – b

2. Theo trên ta có $f(c + d) - f(c) \vdots d$ (1)

$f(c + d) - f(d) \vdots c$ (2)

Nếu $f(c + d) \vdots cd$ thì $f(c + d) \vdots d$, kết hợp với (1) ta được $f(c) \vdots d$

$f(c + d) \vdots cd$ thì $f(c + d) \vdots c$, kết hợp với (2) ta được $f(d) \vdots c$

Ngược lại, nếu $f(c) \vdots d$ và $f(d) \vdots c$ thì từ (1) và (2) suy ra $f(c + d) \vdots c$ và

$f(c + d) \vdots d$, vì (c, d) = 1 nên $f(c + d) \vdots cd$.

Bài 1.17. Gọi x_1, x_2 là nghiệm của phương trình $x^2 - 6x + 1 = 0$. Với mọi số nguyên n, đặt $S_n = x_1^n + x_2^n$, chứng minh rằng S_n là một số nguyên và không chia hết cho 5. *(Trích tài liệu [5])*

Lời giải:

Ta có x_1, x_2 khác 0, $x_1 + x_2 = 6$, $x_1x_2 = 1$.

+ Trường hợp 1: $n \geq 0$

Với n = 0 thì $S_0 = 2$, là số nguyên và không chia hết cho 5.

Với n = 1 thì $S_1 = 6$, là số nguyên và không chia hết cho 5.

Giả sử S_0, S_1, S_2, …, S_{n-1} đều là các số nguyên và không chia hết cho 5. Ta sẽ chứng minh S_n là một số nguyên và không chia hết 5.

Ta có $S_n = x_1^n + x^n_2 = x_1^n + x_2^n + x_1x_2^{n-1} + x_2x_1^{n-1} - x_1x_2^{n-1} - x_2x_1^{n-1}$

$= x_1(x_1^{n-1} + x_2^{n-1}) + x_2(x_1^{n-1} + x_2^{n-1}) - x_1x_2(x_1^{n-2} + x_2^{n-2})$

$= (x_1 + x_2)(x_1^{n-1} + x_2^{n-2}) - x_1x_2(x_1^{n-2} + x_2^{n-2})$

$= 6(x_1^{n-1} + x_2^{n-2}) - (x_1^{n-2} + x_2^{n-2})$

$= 6S_{n-1} - S_{n-2} = 6(6S_{n-2} - S_{n-3}) - S_{n-2} = 35S_{n-2} - 6S_{n-3}.$

Vì S_{n-2}, S_{n-3} là các số nguyên và không chia hết cho 5 nên S_n cũng là số nguyên và không chia hết cho 5.

+ Trường hợp 2: $n < 0$. Đặt $n = -m$, với $m > 0$. Khi đó ta có:

$S_n = x_1^n + x_2^n = x_1^{-m} + x_2^{-m} = \frac{1}{x_1^m} + \frac{1}{x_2^m} = \frac{x_1^m + x_2^m}{x_1^m x_2^m} = \frac{x_1^m + x_2^m}{(x_1x_2)^m} = x_1^m + x_2^m,$

Với $m \geq 0$ nên theo chứng minh trên thì $x_1^m + x_2^m$ là số nguyên và không chia hết cho 5 hay S_n là số nguyên và không chia hết cho 5.

Vậy S_n là số nguyên và không chia hết cho 5 với mọi số nguyên n.

Bài 1.18. (Đề tuyển sinh THPT chuyên ĐHKHTN – ĐHQGHN – 2007, *tài liệu [2]***).** Cho a, b là các số nguyên dương thỏa mãn a + 1 và b + 2007 đều chia hết cho 6. Chứng minh rằng $4^a + a + b$ chia hết cho 6.

Lời giải:

Ta có a + b + 1 + 2007 chia hết cho 6, nên a + b + 2008 chia hết cho 6.

Mà 2010 chia hết cho 6, nên a + b + 2002 – 2010 chia hết cho 6 hay a + b – 2 chia hết cho 6. Do đó a + b + 4 chia hết cho 6 (1)

Mặt khác: $4^a - 4 = 4(4^{a-1} - 1) = 4(4 - 1)(4^{a-2} + 4^{a-3} + \ldots + 4 + 1)$ chia hết cho 12.

Do đó $4^a - 4$ chia hết cho 6 (2).

Từ (1) và (2), ta có $a + b + 4 + 4^a - 4$ chia hết cho 6 hay $4^a + a + b$ chia hết cho 6.

Bài 1.19. (Đề tuyển sinh THPT chuyên Vĩnh Phúc, 2013 – 2014, *tài liệu [2]***).** Chứng minh rằng nếu n là số nguyên dương thì $2(1^{2013} + 2^{2013} + \ldots + n^{2013})$ chia hết cho n(n + 1).

Lời giải:

Ta đã biết a, b là hai số nguyên dương thì $a^{2013} + b^{2013}$ chia hết cho a + b.

Khi đó ta có

$2(1^{2013} + 2^{2013} + \ldots + n^{2013}) = (1^{2013} + n^{2013}) + (2^{2013} + (n-1)^{2013}) + \ldots + (n^{2013} + 1^{2013})$ chia hết cho $n + 1$ (1).

Mặt khác: $2(1^{2013} + 2^{2013} + \ldots + n^{2013}) =$

$(1^{2013} + (n - 1^{2013})) + (2^{2013} + (n-2)^{2013}) + \ldots + ((n-1)^{2013} + 1^{2013})$ chia hết cho n (2)

Do (n, n+1) = 1, kết hợp với (1), (2) ta được $2(1^{2013} + 2^{2013} + \ldots + n^{2013})$ chia hết cho n(n + 1)

Bài 1.20. (Chọn đội tuyển IMO, Hồng Kông, lần 2, 2000; *tài liệu [1]***).** Chứng minh rằng số $n^{30} - n^{18} - n^{14} + n^2$ chia hết cho 46410, với mọi số nguyên n.

Lời giải:

Ta có : $n^{30} - n^{18} - n^{14} + n^2 = n^2(n^{28} - n^{16} - n^{12} + 1) = n^2[n^{12}(n^{16} - 1) - (n^{16} - 1)]$

$= n^2(n^{12} - 1)(n^{16} - 1)$

và 46410 = 2.3.5.7.13.17.

Do đó ta chỉ cần chứng minh số $n^{30} - n^{18} - n^{14} + n^2$ chia hết cho p với p = 2, 3, 5, 7, 13, 17.

Nếu n chia hết cho p thì $n^{30} - n^{18} - n^{14} + n^2$ chia hết cho 46410.

Nếu n không chia hết cho p, tức là (p, n) = 1. Khi đó áp dụng định lí Fecmat nhỏ ta có $n^{p-1} \equiv 1 \pmod p$.

Mà với mỗi p thì số p – 1 là ước của 12 hoặc của 16. Do đó hoặc $(n^{12} - 1)$ chia hết cho p hoặc $n^{16} - 1$ chia hết cho p. Chính vì vậy $n^{30} - n^{18} - n^{14} + n^2$ chia hết cho p, với p = 2, 3, 5, 7, 13, 17.

Vậy $n^{30} - n^{18} - n^{14} + n^2$ chia hết cho 46410.

1.3. Bài toán về ước chung lớn nhất (ƯCLN) và bội chung nhỏ nhất (BCNN)

Bài 1.21. Tìm hai số tự nhiên a, b biết rằng a + b = 128 và (a, b) = 16.

Lời giải:

Vì (a, b) = 16 nên a = 16m, b = 16n với (m, n) = 1.

Vì a + b = 128 nên 16m + 16n = 128 hay m + n = 8.

Vì (m, n) = 1 và m + n = 8 nên ta có 4 trường hợp :

m = 1 và n = 7 thì a = 16 và b = 112.

m = 3 và n = 5 thì a = 48 và b = 80.

m = 5 và n = 3 thì a = 80 và b = 48.

m = 7 và n = 1 thì a = 112 và b = 16.

Vậy ta có 4 đáp án (a, b) = (16, 112); (48, 80); (80, 48); (112, 16).

Bài 1.22. Tìm hai số tự nhiên a, b biết rằng (a, b) = 6 và [a, b] = 36.

Lời giải:

Do vai trò của a và b là như nhau nên không mất tính tổng quát ta giả sử a ≤ b. Áp dụng công thức (a, b).[a, b] = ab, ta có ab = 36.6 = 216.

Vì (a, b) = 6 nên a = 6m, b = 6n, với m ≤ n và (m, n) = 1.

Thay vào ab = 216, ta được 6m.6n = 216, do đó mn = 6. Ta có 2 trường hợp sau:

m = 1 và n = 6 thì a = 6 và b = 36

m = 2 và n = 3 thì a = 12 và b = 18

Vì vai trò của a, b như nhau nên ta có 4 đáp số: (a, b) = (6, 36); (12, 18); (18, 12); (36, 6).

Bài 1.23. Tìm hai số tự nhiên a, b thỏa mãn a + b = 42 và [a, b] = 72.

Lời giải:

Vì vai trò của a, b là như nhau nên ko mất tính tổng quát ta giả sử a ≤ b.

Gọi d = (a, b) thì a = md, b = nd với m, n là 2 số nguyên dương, (m, n) = 1, m ≤ n.

Khi đó a + b = d(m + n) = 42 (1)

[a, b] = mnd = 72 (2).

Do đó d là ước chung của 42 và 72, nên d thuộc tập {1; 2; 3; 6}. Lần lượt thay các giá trị của d vào (1) và (2) ta thấy chỉ có d = 6 là thỏa mãn. Khi đó m + n = 7, m.n = 12, suy ra m = 3, n = 4. Ta tìm được a = 3.6 = 18 và b = 4.6 = 24. Do vai trò của a, b như nhau nên ta có đáp số là (a, b) = (18, 24), (24, 18).

Bài 1.24. Tìm ước chung lớn nhất (a, b) biết a là số gồm 2015 chữ số 2, còn b là số gồm 8 chữ số 2.

Lời giải:

Ta có 2015 chia cho 8 dư 7, còn 8 chia cho 7 dư 1 nên theo Euclid thì

$$(a, b) = (\underbrace{22\ldots22}_{2015\text{ chữ số }2}, \underbrace{22\ldots22}_{8\text{ chữ số }2}) = \left(\underbrace{22\ldots22}_{8\text{ chữ số }2}, \underbrace{22\ldots22}_{7\text{ chữ số }2}\right) = \left(\underbrace{22\ldots22}_{7\text{ chữ số }2}, 2\right) = 2$$

Bài 1.25. Cho số tự nhiên n, chứng tỏ rằng (5n + 6, 6n + 7) = 1

Lời giải:

Giả sử (5n + 6, 6n + 7) = d thì

$$\begin{cases} 5n + 6 \vdots d \\ 6n + 7 \vdots d \end{cases} \Leftrightarrow \begin{cases} 6(5n + 6) \vdots d \\ 5(6n + 7) \vdots d \end{cases} \Leftrightarrow \begin{cases} 30n + 36 \vdots d \\ 30n + 35 \vdots d \end{cases}.$$

Khi đó (30n + 36) – (30n + 35) ⋮ d hay 1 ⋮ d. Vậy (5n + 6, 6n + 7) = 1.

Bài 1.26. Chứng tỏ rằng nếu (a, b) = 1 thì (a – b, a + b) bằng 1 hoặc bằng 2.

Lời giải:

Giả sử d = (a – b, a + b) thì $\begin{cases} a - b \vdots d \\ a + b \vdots d \end{cases} \Leftrightarrow \begin{cases} a - b = md \\ a + b = nd \end{cases}$, với $m, n \in \mathbb{N}$

$$\Leftrightarrow \begin{cases} 2a = md + nd \\ 2b = nd - md \end{cases} \Leftrightarrow \begin{cases} 2a = d(n + m) \\ 2b = d(n - m) \end{cases} \Leftrightarrow \begin{cases} 2a \vdots d \\ 2b \vdots d \end{cases}.$$

Do đó d ∈ ƯC (2a, 2b) hay (2a, 2b) ⋮ d ⇔ 2(a, b) ⋮ d ⇔ 2 ⋮ d (vì (a, b) = 1). Vậy d = 1 hoặc d = 2.

Bài 1.27. Chứng minh rằng nếu (a, b) = 1 và c là ước của a + b thì

(c, a) = (c, b) = 1.

Lời giải:

Giả sử d = (c, a) thì a ⋮ d và c ⋮ d, mà c là ước của a + b nên (c, b) = d hay b ⋮ d. Từ đó ta có (a, b) = d = 1. Vậy (c, a) = (c, b) = 1.

Bài 1.28. Chứng tỏ rằng nếu (a, c) = (a, b) = 1 thì (a, bc) = 1. Tổng quát hơn, nếu $(a_1, b) = (a_2, b) = \ldots = (a_n, b) = 1$ thì $(a_1a_2\ldots a_n, b) = 1$.

Lời giải:

Giả sử (a, bc) = d là số nguyên tố. Khi đó a ⋮ d và bc ⋮ d hay a⋮ d và b ⋮ d (vô lí vì (a, b) = 1) hoặc a ⋮ d và c ⋮ d (vô lí vì (a, c) = 1). Vậy (a, bc) = 1.

Tổng quát : Giả sử $(a_1a_2\ldots a_n, b) = d$ là số nguyên tố thì $a_1a_2\ldots a_n \vdots d$ và b ⋮ d hay

$a_1 \vdots d$ và b ⋮ d (vô lí vì $(a_1, b) = 1$)

hoặc $a_2 \vdots d$ và b ⋮ d (vô lí vì $(a_2, b) = 1$)

.

.

.

hoặc $a_n \vdots d$ và b ⋮ d (vô lí vì $(a_n, b) = 1$).

Vậy $(a_1a_2\ldots a_n, b) = 1$.

Bài 1.29. Tìm bội chung nhỏ nhất [n, n + 1, n + 2]

Lời giải:

Đặt A = [n, n + 1], B = [[n, n + 1], n + 2].

Áp dụng tính chất [a, b, c] = [[a, b], c], ta có: B = [n, n + 1, n + 2]

Dễ thấy (n, n + 1) = 1 nên [n, n + 1] = n(n + 1)

Áp dụng công thức [a, b](a, b) = ab, suy ra [a, b] = $\frac{ab}{(a,b)}$.

Khi đó [n, n + 1, n + 2] = $\frac{n(n+1)(n+2)}{(n(n+1),n+2)}$. Do (n + 1, n + 2) = 1,

gọi d = (n, n + 2) = (n, 2) thì [n, n + 1, n + 2] = $\frac{n(n+1)(n+2)}{d}$.

Nếu n chẵn thì d = 2. Khi đó [n, n + 1, n + 2] = $\frac{n(n+1)(n+2)}{2}$.

Nếu n lẻ thì d = 1. Khi đó [n, n + 1, n + 2] = n(n + 1)(n + 2)

Bài 1.30. Chứng minh rằng nếu m, n là các số tự nhiên, m lẻ thì

$$(2^m - 1, 2^n + 1) = 1.$$

Lời giải:

Gọi d = $(2^m - 1, 2^n + 1)$. Khi đó d lẻ và $2^m - 1 = kd$, $2^n + 1 = ld$ với l, k là các số tự nhiên. Vì vậy $2^m = kd + 1$, $2^n = ld - 1$.

Từ đó ta có $2^{mn} = (kd + 1)^n = ud + 1$ và $2^{mn} = (ld - 1)^n = vd - 1$, với u, v là hai số tự nhiên. Do đó ud + 1 = vd – 1, do đó d là ước của 2, mà d lẻ nên d = 1.

Vậy $(2^m - 1, 2^n + 1) = 1$.

Bài 1.31. Tìm ƯCLN (n ! + 1, (n + 1) ! + 1), với mọi số tự nhiên n.

Lời giải :

Gọi d = (n ! + 1, (n + 1) ! + 1)

Ta có (n ! + 1)(n + 1) = (n + 1) ! + n + 1. Do d là ước của n ! + 1 nên d là ước của (n ! + 1)(n + 1) hay d là ước của (n + 1) ! + n + 1.

Mà d lại là ước của (n + 1) ! + 1 nên d là ước của n, kết hợp với d là ước của n ! + 1, ta được d là ước của 1 hay d = 1.

Vậy (n ! + 1, (n + 1) ! + 1) = 1

Bài 1.32. Cho a, m là các số tự nhiên lớn hơn 1. Chứng minh rằng

$(1 + a + a^2 + \dots a^{m-1}, a - 1) = (m, (a - 1))$.

Lời giải:

Nếu $d = (1 + a + a^2 + \dots a^{m-1}, a - 1)$. Khi đó $1 + a + a^2 + \dots a^{m-1} \vdots d$ hay

$(a^{m-1} - 1) + (a^{m-2} - 1) + \dots + (a - 1) + m \vdots d$. Mà $a - 1 \vdots d$, do đó $m \vdots d$. Vậy d là ước của $a - 1$ và m.

Ngược lại, nếu d là ước của $a - 1$ và m thì d là ước của

$(a^{m-1} - 1) + (a^{m-2} - 1) + \dots + (a - 1) + m$ hay d là ước của $1 + a + a^2 + \dots a^{m-1}$.

Vậy $(1 + a + a^2 + \dots a^{m-1}, a - 1) = (m, (a - 1))$.

Bài 1.33. Cho $(m, n) = 1$, tìm

a. $(m + n, m^2 + n^2)$

b. $(mn, m^2 + n^2)$

Lời giải:

a. Giả sử $d = (m + n, m^2 + n^2)$. Khi đó d là ước của $m + n$ và d là ước của $m^2 + n^2$, Từ đó ta có d là ước của $(m + n)^2 - (m^2 + n^2) = 2mn$.

d là ước của $m + n$ và d là ước của $2mn$ thì d cũng là ước của $2m(m + n) - 2mn = 2m^2$ và d là ước của $2n(m + n) - 2mn = 2n^2$. Do đó d là ước của $(2m^2, 2n^2) = 2(m^2, n^2) = 2$. suy ra $d = 1$ hoặc $d = 2$.

Vậy $(m + n, m^2 + n^2) = 1$ khi m, n khác tính chẵn, lẻ

$(m + n, m^2 + n^2) = 2$ khi m, n cùng lẻ.

b. Giả sử $d = (mn, m^2 + n^2)$. Khi đó d là ước của mm và d là ước của $m^2 + n^2$, suy ra d là ước của $m(m^2 + n^2) - mn^2 = m^3$ và d là ước của $n(m^2 + n^2) - nm^2 = n^3$. Do đó d là ước của $(m^3, n^3) = 1$. Vậy $(mn, m^2 + n^2) = 1$.

Bài 1.34. Tìm ƯCLN $(a^m - 1, a^n - 1)$ với a là số nguyên sao cho $a(a^2 - 1)$ khác 0 và m, n là các số tự nhiên.

Lời giải:

Đặt $d = (m, n)$ thì $a^m - 1 \vdots a^d - 1$ và $a^n - 1 \vdots a^d - 1$, ta sẽ chứng minh khẳng định này.

Thật vậy, $m = kd$ $(k \in \mathbb{N})$ thì

$a^m - 1 = a^{kd} - 1 = (a^d)^k - 1 = (a^d - 1)((a^d)^{k-1} + (a^d)^{k-2} + \dots + 1) \vdots a^d - 1$

Tương tự ta chứng minh được $a^n - 1 \vdots a^d - 1$

Giả sử $(a^m - 1, a^n - 1) = A$ thì A có dạng $b(a^d - 1)$. Ta tìm b:

Với

a	2	3	4
m	2	3	4
n	4	5	6
A	3	2	15
b	1	1	1

Dự đoán $(a^m - 1, a^n - 1) = A = a^{(m,n)} - 1$.

Do $A \vdots a^{(m,n)} - 1$ nên để chứng minh $A = a^{(m,n)} - 1$, ta chứng minh $a^{(m,n)} - 1 \vdots A$:

Tồn tại các số nguyên dương x, y sao cho $xm + yn = (m, n)$

hay $xm - yn = (m, n)$ hay $-xm + yn = (m, n)$.

Xét trường hợp $xm - yn = (m, n)$, các trường hợp khác làm tương tự.

Ta có $a^{yn}(a^{xm-yn} - 1) = a^{xm} - a^{yn} = (a^{xm} - 1) - (a^{yn} - 1) = (a^m - 1)C - (a^n - 1)D \vdots A$.

Mà $(a^{yn}, a^n - 1) = 1$ nên $(a^{yn}, A) = 1$. Do đó $a^{xm-yn} - 1 = a^{(m,n)} - 1 \vdots A$.

Vậy $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Bài 1.35. (OM Baltic, 2001, *tài liệu [1]***).** Cho a là số nguyên dương lẻ và m, n là hai số nguyên dương phân biệt. Chứng minh rằng $(a^{2^n} + 2^{2^n}, a^{2^m} + 2^{2^m}) = 1$.

Lời giải:

Vì vai trò của m, n là như nhau nên không mất tính tổng quát ta giả sử $m > n > 0$.

Gọi p là ước nguyên tố của $a^{2^n} + 2^{2^n}$ thì $a^{2^n} \equiv -2^{2^n} \pmod p$. Bình phương hai vế lên $m - n$ lần ta được $a^{2^n.2^{m-n}} \equiv 2^{2^n.2^{m-n}} \pmod p \Leftrightarrow a^{2^m} \equiv 2^{2^m} \pmod p$. Cộng cả hai vế với 2^{2^m} ta được $a^{2^m} + 2^{2^m} \equiv 2.2^{2^m} \pmod p$. Do đó $a^{2^m} + 2^{2^m}$ không chia hết cho p.

Vậy $(a^{2^n} + 2^{2^n}, a^{2^m} + 2^{2^m}) = 1$.

1.4. Bài toán về số nguyên tố

Bài 1.36. Chứng minh rằng có vô số số nguyên tố.

Lời giải :

Giả sử có hữu hạn số nguyên tố $p_1 , p_2 , \dots , p_n$ trong đó số p_n là lớn nhất.

Xét số A = $p_1p_2\ldots p_n + 1$. Khi đó A chia cho mỗi số nguyên tố p_i ($1 \le i \le n$) đều dư 1 (1).

Mà A lớn hơn p_n nên A là hợp số (2).

Ta thấy (1) và (2) mâu thuẫn.

Vậy có vô số số nguyên tố.

Bài 1.37. Chứng minh rằng với mọi số nguyên dương n đều tồn tại n số tự nhiên liên tiếp là hợp số.

Lời giải :

Lấy số B = 2.3.4…n(n + 1) = (n + 1) !

Khi đó ta có : B + 2 chia hết cho 2 nên B + 2 là hợp số

B + 3 chia hết cho 3 nên B + 3 là hợp số

….

B + (n + 1) chia hết cho n + 1 nên B + n + 1 là hợp số

Vậy tồn tại n số tự nhiên liên tiếp (n + 1) ! + 2, (n + 1) ! + 3, …, (n + 1) ! + n + 1 là hợp số.

Bài 1.38. Chứng minh rằng số A = $\frac{5^{125}-1}{5^{25}-1}$ không phải là số nguyên tố.

(Trích tài liệu [5])

Lời giải :

Đặt 5^{25} = x, ta được số $\frac{a^5-1}{a-1} = a^4 + a^3 + a^2 + a + 1$

$= a^4 + 9a^2 + 1 + 6a^3 + 2a^2 + 6a - 10a^2 - 5a^3 - 5a$

$= (a^2 + 3a + 1)^2 - 5a(a^2 + 2a + 1)$

$= (a^2 + 3a + 1)^2 - 5^{26}(a + 1)^2$

$= (a^2 + 3a + 1)^2 - (5^{13}a + 5^{13})^2$

$= (a^2 + 3a + 1 - 5^{13}a - 5^{13})(a^2 + 3a + 1 + 5^{13}a + 5^{13})$

Vì $\frac{a^5-1}{a-1}$ là tích hai số nên nó là hợp số hay $\frac{5^{125}-1}{5^{25}-1}$ không là số nguyên tố.

Bài 1.39. Cho a = $\underbrace{11\ldots11}_{2014\text{ số}}$, a có phải số nguyên tố không ?

Lời giải:

Vì số 1 lập lại 2014 lần nên số 11 (2 số 1 liên tiếp) lập lại 2014 : 2 = 1007 lần. Do đó a = $11.\underbrace{0101\ldots01}_{1007\text{ số }01}$, vì số 11 nhân với mỗi số 01 sẽ được số 11 nên khi có 1007 số 01 viết liên tiếp nhân với 11 sẽ ra số gồm 1007 chữ số 11 viết liên tiếp. Vậy a chia hết cho 11 nên a là hợp số.

Bài 1.40. Chứng minh rằng mọi ước số nguyên tố của 2014! – 1 đều lớn hơn 2014.

Lời giải:

Gọi p là ước số nguyên tố của 2014! – 1

Giả sử $p \leq 2014$, thì 2014! chia hết cho p. Mà 2014! – 1 cũng chia hết cho p nên 1 chia hết cho p, điều này là vô lí. Vậy $p > 2014$.

Bài 1.41. Tìm số nguyên tố p để $p^3 – 6$, $2p^3 + 5$ và $p^2 + 10$ là các số nguyên tố.

(Trích tài liệu [6])

Lời giải:

Nếu p = 7 thì $p^3 – 6 = 337$, $2p^3 + 5 = 691$ và $p^2 + 10 = 59$ đều là các số nguyên tố.

Nếu p là số nguyên tố khác 7 thì p^3 chia 7 cho số dư là 1 hoặc 6. Khi đó thì $2p^3 + 5$ hoặc $p^3 – 6$ chia hết cho 7 nên không thỏa mãn.

Vậy với p = 7 thì $p^3 – 6$, $2p^3 + 5$ và $p^2 + 10$ là các số nguyên tố.

Bài 1.42. Tìm các số nguyên tố p, q sao cho 7p + q và pq + 17 đều là các số nguyên tố.

Lời giải :

Dễ thấy p và q có một số chẵn hoặc có một số lẻ.

+) Nếu p chẵn mà p là số nguyên tố nên p = 2.

Xét q = 3k, vì q là số nguyên tố nên q = 3. Ta có: 7p + q = 14 + 3 = 17 (là số nguyên tố) và pq + 17 = 6 + 17 = 23 (là số nguyên tố)

Xét q = 3k + 1. Ta có: 7p + q = 14 + 3k + 1 = 15 + 3k ⋮ 3 (là hợp số, loại)

Xét q = 3k + 2. Ta có: pq + 17 = 2(3k + 2) + 17 = 6k + 4 + 17 = 6k + 21 ⋮ 3 (là hợp số, loại)

Vậy p = 2, q = 3.

+) Nếu q chẵn mà q là số nguyên tố nên q = 2.

Xét p = 3k, vì p là số nguyên tố nên p = 3. Ta có: 7p + q = 21 + 2 = 23 (là số nguyên tố) và pq + 17 = 23 (là số nguyên tố)

Xét p = 3k + 1. Ta có: 7p + q = 7(3k + 1) + 2 = 21k + 9 ⋮ 3 (là hợp số, loại)

Xét p = 3k + 2. Ta có: pq + 17 = 2(3k + 2) + 17 = 6k + 4 + 17 = 6k + 31 ⋮ 3 (là hợp số, loại)

Do đó q = 2, p = 3.

Vậy để 7p + q và pq + 17 đều là các số nguyên tố thì q = 2, p = 3 hoặc q = 3, p = 2

Bài 1.43. Tìm ba số nguyên tố p, q, r thỏa mãn $p^q + q^p = r$.

Lời giải:

Vì p và q là hai số nguyên tố nên $p^q + q^p > 2$, do đó r > 2, mà r cũng là số nguyên tố nên r lẻ và $p^q + q^p$ cũng lẻ, do đó trong 2 số p và q phải có 1 số lẻ, 1 số chẵn, hay p = 2 hoặc q = 2.

+) Nếu p = 2 , đặt q = 2k + 1 ($k \in \mathbb{N}^*$)

Xét q = 3 thì $r = 2^3 + 3^2 = 17$ (thỏa mãn)

Xét q > 3. Ta có $2^q = 2^{2k+1}$, nên $2^q - 2 = 2^{2k+1} - 2 = 2.4^k - 2 = 2(4^k - 1)$

$= 2.(4 - 1)(4^{k-1} + 4^{k-2} + \ldots + 1)$ chia hết cho 3. Vậy $2^q = 3n + 2$ ($n \in \mathbb{N}^*$).

Vì q là số nguyên tố và q > 3 nên $q = 3a \pm 1$ ($a \in \mathbb{N}^*$),

do đó $q^2 = (3a \pm 1)^2 = 9a^2 \pm 6a + 1 = 3m + 1$ ($m \in \mathbb{N}^*$)

Mà $2^q + q^2 = r$ nên $r = 3n + 2 + 3m + 1 = 3(n + m + 1)$ chia hết cho 3 (không thỏa mãn)

+) Nếu q = 2, làm tương tự trường hợp trên ta được q = 2, p = 3, r = 17.

Vậy ta có 2 bộ số thỏa mãn đề bài là (2, 3, 27) và (3, 2, 17)

Bài 1.44. Xác định tất cả các số nguyên n để $n^4 + 4^n$ không những là số nguyên mà còn là số nguyên tố. *(Trích tài liệu [6])*

Lời giải :

Trường hợp 1: n < 0, ta có n^4 là số nguyên nhưng 4^n không phải số nguyên, do đó $n^4 + 4^n$ không là số nguyên (loại).

Trường hợp 2: n = 0, ta có $n^4 + 4^n = 1$, không là số nguyên tố.

Trường hợp 3: n = 1, ta có $n^4 + 4^n = 1^4 + 4^1 = 5$, là số nguyên tố.

Trường hợp 4: $n \geq 2$, xét 2 trường hợp:

· Trường hợp 4a: n chẵn.

Khi đó $n^4 + 4^n$ chia hết cho 2, mặt khác $n^4 + 4^n > 2$ (vì $n \geq 2$) nên $n^4 + 4^n$ không là số nguyên tố.

· Trường hợp 4b: n lẻ. Đặt $n = 2k + 1$ (k là số nguyên dương).

Ta có $n^4 + 4^n = n^4 + 2.n^2.2^{2k+1} + 4^{2k+1} - n^2.2^{2k+2} = (n^2 + 2^{2k+1})^2 - n^2.2^{2k+2}$

$= (n^2 + 2^{2k+1} - n.2.2^k)(n^2 + 2^{2k+1} + n.2.2^k)$.

Vì $n \geq 2$ nên $n^2 + 2^{2k+1} + n.2.2^k > 1$

Mặt khác theo bất đẳng thức AM-GM, ta có:

$n^2 + 2^{2k+1} \geq 2.n.2^k.\sqrt{2} > 2.n.2^k$ hay $n^2 + 2^{2k+1} - n.2.2^k > 1$

Do đó $n^4 + 4^n$ không là số nguyên tố

Vậy với $n = 1$ thì $n^4 + 4^n$ là số nguyên tố.

Bài 1.45. Tìm số nguyên tố p thoả mãn $p^3 - 4p + 9$ là số chính phương. *(Trích tài liệu [6])*

Lời giải:

Đặt $p^3 - 4p + 9 = t^2$ (t là số tự nhiên)

Biến đổi thành: $p(p^2 - 4) = (t - 3)(t + 3)$ (1).

Do đó p là ước của $(t - 3)$ hoặc p là ước của $(t + 3)$

+) Nếu p là ước của $t - 3$. Đặt $t - 3 = pk$ ($k \in \mathbb{N}$)

Khi đó thay vào (1), ta được :

$p(p^2 - 4) = pk.(t + 3)$ hay $k(t + 3) = p^2 - 4 \Rightarrow p^2 = kt + 3k + 4$

Mặt khác có

$(t - 3)^2 = p^2k^2 \Leftrightarrow t^2 - 6t + 9 = k^2(kt + 3k + 4) \Leftrightarrow t^2 - t(6 + k^3) + 9 - 3k^3 - 4k^2 = 0$

Coi đây là phương trình bậc hai ẩn t, điều kiện cần để tồn tại nghiệm nguyên của phương trình là :

$\Delta = (6 + k^3)^2 - 4(9 - 3k^3 - 4k^2) = k^6 + 24k^3 + 16k^2 = k^2(k^4 + 24k + 16)$ là một số chính phương. Muốn vậy thì $k^4 + 24k + 16$ phải là một số chính phương.

Mặt khác với $k > 3$, ta dễ chứng minh được $(k^2)^2 < k^4 + 24k + 16 < (k^2 + 4)^2$. Suy ra các trường hợp

$k^4 + 24k + 16 = (k^2 + 1)^2 \Leftrightarrow 2k^2 - 24k - 15 = 0$ (loại vì không có nghiệm nguyên)

$k^4 + 24k + 16 = (k^2 + 2)^2 \Leftrightarrow 4k^2 - 24k - 12 = 0$ (loại)

$k^4 + 24k + 16 = (k^2 + 3)^2 \Leftrightarrow 6k^2 - 24k - 7 = 0$ (loại)

Do đó phải có $k \leq 3$, thử trực tiếp được $k = 3$ thỏa mãn. Từ đó tìm được $t = 36$, $p = 1$

+) Nếu p là ước của $t + 3$. Đặt $t + 3 = pk$ ($k \in N$).

Khi đó thay vào (1), được :

$p(p^2 - 4) = pk(t - 3) \Rightarrow p^2 = kt - 3k + 4$

Mặt khác, ta có

$(t + 3)^2 = p^2k^2 \Leftrightarrow t^2 + 6t + 9 = k^2(kt - 3k + 4) \Leftrightarrow t^2 + (6 - k^3)t + 9 + 3k^3 - 4k^2 = 0$

Coi đây là phương trình bậc hai ẩn t, điều kiện cần để tồn tại nghiệm nguyên của phương trình trên là :

$\Delta = (6 - k^3)^2 - 4(9 + 3k^3 - 4k^2) = k^2(k^4 - 24k + 16)$ là số chính phương.

Muốn vậy thì $k^4 - 24k + 16$ phải là số chính phương.

Mặt khác ta dễ chứng minh được rằng với $k > 3$ thì $(k^2 - 4)^2 < k^4 - 24k + 16 < (k^2)^2$.

Suy ra các trường hợp :

$k^4 - 24k + 16 = (k^2 - 1)^2 \Leftrightarrow 2k^2 - 24k + 15 = 0$ (loại)

$k^4 - 24k + 16 = (k^2 - 2)^2 \Leftrightarrow 4k^2 - 24k + 12 = 0$ (loại)

$k^4 - 24k + 16 = (k^2 - 3)^2 \Leftrightarrow 6k^2 - 24k + 7 = 0$ (loại)

Do đó $k \leq 3$. Thử trực tiếp thấy $k = 3$ thỏa mãn, khi đó $t = 3; 18$, tương ứng $p = 2; 7$

Vậy $p \in \{2; 7; 11\}$

Bài 1.46. Tìm các số nguyên tố p sao cho $13p + 1$ là lập phương của một số tự nhiên.

Lời giải:

Đặt $13p + 1 = k^3$ (k là số tự nhiên), khi đó $13p = k^3 - 1 = (k - 1)(k^2 + k + 1)$. Từ đó ta suy ra 13 là ước của $k - 1$ hoặc 13 là ước của $k^2 + k + 1$.

Nếu 13 là ước của $k - 1$ thì $k = 14$, khi đó $p = 211$ (vì nếu $k > 14$ thì p là tích của 2 số)

Nếu 13 là ước của $k^2 + k + 1$ thì $k^2 + k + 1 = 13$, khi đó $k = -4$ (loại); $k = 3$ thì $p = 2$.

Vậy $p = 2$ hoặc $p = 211$.

Bài 1.47. Tìm các số tự nhiên m, n để $Q = 3^{3m^2+6n-61} + 4$ là số nguyên tố.

Lời giải :

Ta có $3m^2 + 6n - 61 = 3(m^2 + 2n - 21) + 2 = 3k + 2$ ($k \in \mathbb{N}^*$).

Khi đó $Q = 3^{3k+2} + 4 = 27^k.9 + 4$. Mà 27 chia cho 13 dư 1 thì $27^k.9$ chia cho 13 dư 9 nên Q chia hết cho 13, kết hợp với giả thiết Q là số nguyên tố, ta được Q = 13, cho nên $m^2 + 2n = 21$, suy ra $m^2 < 21$ và m lẻ nên m = 1 hoặc m = 3.

Vậy ta tìm được 2 cặp số là (1, 10) và (3, 6).

Bài 1.48. Tìm số nguyên dương n để $M = n^{2015} + n^{2014} + 1$ là số nguyên tố.

Lời giải:

Ta có $M = n^{2015} + n^{2014} + 1 = n^2(n^{2013} - 1) + n(n^{2013} - 1) + n^2 + n + 1$

Với n > 1, ta có: $n^{2013} - 1 \vdots n^3 - 1 \vdots n^2 + n + 1$ và $n^2 + n + 1 > 1$ nên M là hợp số

Với n = 1 thì M = 3 là số nguyên tố.

Vậy với n = 1 thì $M = n^{2015} + n^{2014} + 1$ là số nguyên tố.

Bài 1.49. Tìm ba số nguyên tố liên tiếp p, q, r sao cho $p^2 + q^2 + r^2$ là số nguyên tố.

Lời giải :

Nếu các số nguyên tố p, q, r đều khác 3 thì p, q, r có dạng $3k \pm 1$.

Khi đó p^2, q^2, r^2 chia cho 3 đều dư 1 nên $p^2 + q^2 + r^2$ chia hết cho 3 nên là hợp số. Do đó một trong ba số phải có một số là 3, các số còn lại là 5, 7 và $p^2 + q^2 + r^2 = 83$ là số nguyên tố

Vậy ba số cần tìm là 3, 5, 7.

Bài 1.50. Tìm tất cả các bộ số nguyên tố (a, b, c) sao cho abc < ab + bc + ca.

Lời giải :

Vì a, b, c có vai trò như nhau nên không mất tính tổng quát ta giải sử $a \le b \le c$. Khi đó

$ab + bc + ca \le 3bc$, kết hợp với giả thiết ta có abc < 3bc, từ đó ta được a < 3, mà a là số nguyên tố nên a = 2

Với a = 2 ta có 2bc < 2b + 2c + bc nên $bc < 2(b + c) \le 4c$, suy ra b < 4, mà b là số nguyên tố nên b = 2 hoặc b = 3.

Nếu b = 2 thì 4c < 2 + 4c, thỏa mãn đề bài với mọi c = p là số nguyên tố.

Nếu b = 3 thì 6c < 6 + 5c, hay c < 6, mà c là số nguyên tố và c ≥ b nên c = 3 hoặc c = 5.

Vậy các bộ số (a, b, c) cần tìm là (2, 2, p), (2, 3, 3), (2, 3, 5) và các hoán vị của chúng, với p là số nguyên tố.

Bài 1.51. Tìm 2011 số nguyên tố sao cho tích các số nguyên tố này bằng tổng các lũy thừa bậc 2010 của chúng.

Lời giải :

Gọi các số nguyên tố cần tìm là $p_1, p_2, \ldots, p_{2011}$. Theo giả thiết ta có :

$p_1p_2\ldots p_{2011} = p_1^{2010} + p_2^{2010} + \ldots + p_{2011}^{2010}$

Gọi k là các số p_i khác 2011 ($0 \leq k \leq 2011$)

Nếu k = 0, khi đó $p_1 = p_2 = \ldots = p_{2011} = 2011$ (thỏa mãn)

Nếu k = 2011, thì $(p_i, 2011) = 1$, với mọi i. Khi đó p^{2010} chia cho 2011 dư 1 nên vế trái chia hết cho 2011 mà vế phải của (1) lại không chia hết cho 2011. Do đó trường hợp này không xảy ra.

Nếu 0 < k < 2011 thì có k số p_i khác 2011 và có 2011 – k số p_i là 2011. Khi đó vế trái của (1) chia cho 2011 dư k, còn vế phải của (1) chia hết cho 2011. Do đó trường hợp này không xảy ra.

Vậy 2011 số nguyên tố cần tìm là $p_1 = p_2 = \ldots = p_{2011} = 2011$.

Bài 1.52. (Đề thi HSG lớp 9 TP Hà Nội, 2013 - 2014). Tìm số tự nhiên n để $5^{2n^2-6n+2} - 12$ là số nguyên tố. *(Trích tài liệu [2])*

Lời giải :

Ta có $2n^2 - 6n + 2 = 2[n(n - 3) + 1]$. Vì n(n – 3) là số chẵn với mọi số tự nhiên n nên n(n – 3) + 1 là số lẻ.

Đặt n(n – 3) + 1 = 2k + 1, với k là số tự nhiên thì

$5^{2n^2-6n+2} - 12 = 25^{2k+1} - 12 = 25^{2k+1} + 1 - 13$. Mà $25^{2k+1} + 1$ chia hết cho (25 + 1) nên $25^{2k+1} + 1 - 13$ chia hết cho 13.

Do đó để $5^{2n^2-6n+2} - 12$ là số nguyên tố thì $5^{2n^2-6n+2} - 12 = 13$, suy ra $2n^2 - 6n + 2 = 2$. Khi đó n = 0 hoặc n = 3.

Vậy với n = 0 hoặc n = 3 thì $5^{2n^2-6n+2} - 12$ là số nguyên tố.

Bài 1.53. (Đề tuyển sinh THPT – ĐHKHTN – ĐHQG Hà Nội _ 2009). Tìm số nguyên dương n sao cho tất cả các số n + 1, n + 3, n + 7, n + 13, n + 17, n + 25, n + 37 đều là số nguyên tố. *(Trích tài liệu [2])*

Lời giải:

Xét n = 7k ($k \geq 1$), không thỏa mãn vì n + 7 = 7k + 7 > 7 và chia hết cho 7

Xét n = 7k + 1 ($k \geq 0$), không thỏa mãn vì n + 13 = 7k + 14 > 7 và chia hết cho 7

Xét n = 7k +2 ($k \geq 1$), không thỏa mãn vì n + 5 = 7k + 7 > 7 và chia hết cho 7, với k = 0 thì n = 2, khi đó n + 7 = 9, không là số nguyên tố

Xét n = 7k + 3 ($k \geq 0$), không thỏa mãn vì n + 25 = 7k + 28 > 7 và chia hết cho 7

Xét n = 7k + 4 ($k \geq 0$), không thỏa mãn vì n + 17 = 7k + 21 > 7 và chia hết cho 7

Xét n = 7k + 5 ($k \geq 0$), không thỏa mãn vì n + 37 = 7k + 42 > 7 và chia hết cho 7

Xét n = 7k + 6 ($k \geq 1$), không thỏa mãn vì n + 1 = 7k + 7 > 7 và chia hết cho 7, với k = 0 thì n = 6, khi đó n + 1 = 7, n + 5 = 11, n + 7 = 13, n + 13 = 19, n + 17 = 23, n + 25 = 31, n + 37 = 43 đều là số nguyên tố.

Vậy với n = 6 thì các số n + 1, n + 3, n + 7, n + 13, n + 17, n + 25, n + 37 đều là số nguyên tố.

Bài 1.54. (MO Nga, 2000). Tìm các số nguyên tố p và q sao cho $p + q = (p - q)^3$ *(Trích tài liệu [1])*

Lời giải:

Theo đề bài ta có $p + q = (p - q)^3$ nên p khác q.

Khi đó $p - q \equiv 2p \pmod{p + q}$ hay $(p – q)^3 \equiv 8p^3 \pmod{p + q}$, suy ra

$8p^3 \equiv 0 \pmod{p + q}$.

Do (p, q) = 1 nên (p, p + q) = 1 suy ra $(p^3, p + q) = 1$. Vậy 8 chia hết cho p + q, khi đó $p + q \leq 8$, mà $p, q \geq 2$ nên $2 \leq q < p \leq 8$, ta tìm được (p, q) = (5, 3).

Bài 1.55. (Chọn đội tuyển IMO của Hồng Kông, 2000). Xác định tất cả các số nguyên tố có dạng $n^n + 1$ và nhỏ hơn 10^{19}, với n là số nguyên dương.

(Trích tài liệu [1])

Lời giải:

Vì $16^{16} + 1 > 2^{64} = 2^4.(2^{10})^6 > 16.1000^6 = 1{,}6.10^{19} > 10^{19}$ nên n < 16.

Giả sử n = mk với k lẻ lớn hơn 1 thì ta có:

$n^n + 1 = n^{mk} + 1 = (n^k + 1)(n^{(m-1)k} – n^{(m-2)k} + n^{(m-3)k} - … + n^{2k} – n^k + 1)$, và

$n^k + 1 > 1$, do đó $n^n + 1$ không phải là số nguyên tố.

Chính vì thế, để $n^n + 1$ là số nguyên tố thì n phải là lũy thừa của 2. Thử các giá trị của n, ta có:

$1^1 + 1 = 2$, $2^2 + 1 = 5$, $4^4 + 1 = 257$ là các số nguyên tố, $8^8 + 1 = (2^8)^3 + 1$ không phải số nguyên tố vì nó chia hết cho $2^8 + 1$.

Vậy các số nguyên tố có dạng $n^n + 1$ và nhỏ hơn 10^{19}, với n là số nguyên dương là 2, 5, 257.

Chương 2. Đồng dư

2.1. Kiến thức cơ bản

2.1.1. Khái niệm đồng dư

Giả sử m là số nguyên dương và a, b là các số nguyên. Chúng ta sẽ nói a đồng dư với b modulo m nếu m là ước của $(a - b)$.

Nếu a đồng dư với b modulo m, ta viết $a \equiv b \pmod{m}$. Ngược lại, ta nói a không đồng dư với b modulo m, kí hiệu $a \not\equiv b \pmod{m}$.

Dễ dàng thấy rằng, $a \equiv b \pmod{m}$ khi và chỉ khi có số nguyên k sao cho $a = b + km$.

Định lý 2.1.1. Đồng dư modulo m là quan hệ tương đương trên $\mathbb{Z}$, tức là có các tính chất :

1. Phản xạ: $a \equiv a \pmod{m}$;
2. Đối xứng $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.
3. Bắc cầu: $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Định lý 2.1.2. Giả sử a, b, c, m là các số nguyên, $m > 0$ và $a \equiv b \pmod{m}$.

Khi đó:

1. $a + c \equiv b + c \pmod{m}$
2. $a - c \equiv b - c \pmod{m}$
3. $ac \equiv bc \pmod{m}$

Chú ý là: từ hệ thức $ac \equiv bc \pmod{m}$, nói chung không thể suy ra $a \equiv b \pmod{m}$; chẳng hạn $6.2 \equiv 1.2 \pmod{10}$, nhưng 6 không đồng dư với 1 (mod 10). Tuy nhiên ta cũng có định lý sau.

Định lý 2.1.3. Nếu $ac \equiv bc \pmod{m}$, $d = (c, m)$ thì $a \equiv b \pmod{m/d}$. Đặc biệt, nếu $ac \equiv bc \pmod{m}$, $(c, m) = 1$ thì $a \equiv b \pmod{m}$

Định lý 2.1.4. Nếu $a \equiv b \pmod{m}$ và $c \equiv d \pmod{m}$ thì:

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$.

Hệ quả 2.1.1. Các phép đồng dư có thể nâng lên lũy thừa, nghĩa là, nếu $a \equiv b \pmod m$ thì với mọi số nguyên không âm n đều có $a^n \equiv b^n \pmod m$

Định lý 2.1.5. Nếu $m_1, m_2, \dots m_k$ là các số nguyên dương và $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ... , $a \equiv b \pmod{m_k}$ thì $a \equiv b \pmod{[m_1, m_2, \dots m_k]}$

Định lí 2.1.6. Nếu $ac \equiv bc \pmod m$ và $(c, m) = 1$ thì $a \equiv b \pmod m$

Định lí 2.1.7. Nếu $a \equiv b \pmod m$ thì :

+ $ac \equiv bc \pmod{bc}$, với c là số nguyên dương.

+ $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, với d là ƯCLN của a, b, m,

2.1.2. Định lý phần dư Trung Hoa

Định lý 2.1.6. Định lý phần dư Trung Hoa. Giả sử $m_1, m_2, \dots m_k$ là các số nguyên dương đôi một nguyên tố cùng nhau. Khi đó hệ các đồng dư

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Có duy nhất nghiệm modulo $M = m_1 m_2 \dots m_k$.

Chứng minh: Đặt $M_j = M/m_j, 1 \le j \le k$. Khi đó, do $(M_j, m_j) = 1$ nên có số nguyên y_j thỏa đồng dư $M_j y_j \equiv 1 \pmod{m_j}$. Đặt

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_k M_k y_k.$$

Do $m_j | M_i$, với mọi $i \ne j$, nên: $x \equiv a_j M_j y_j \equiv a_j \pmod{m_j}$ $1 \le j \le k$.

Bây giờ ta giả sử x_1, x_2 là các nghiệm của hệ. Thế thì với mọi $j, 0 \le j \le k$, ta đều có $x_1 \equiv x_2 \pmod{m_j}$. Suy ra , với mọi $j, 0 \le j \le k, m_j \mid (x_1 - x_2)$. Vì các số $m_1, m_2, \dots m_k$ đôi một nguyên tố cùng nhau nên $M = m_1, m_2, \dots m_k \mid (x_1 - x_2)$; hay $x_1 \equiv x_2 \pmod M$.

2.1.3. Định lý Wilson và định lý Euler

Định lý 2.1.7. Định lý Wilson. Nếu p là số nguyên tố thì $(p-1)! \equiv -1 \pmod{p}$.

Chứng minh: Định lý là đúng trong trường hợp $p = 2, 3$. Ta xét trường hợp $p > 3$.

Đối với mỗi số nguyên $a, 2 \leq a \leq p-2$, do $(a, p) = 1$ nên a có nghịch đảo duy nhất $\bar{a}$ modulo p: $1 \leq \bar{a} \leq p-1$. Mặt khác, $a \neq \bar{a}$, vì nếu không thì $a^2 \equiv 1 \pmod{p}$, suy ra $(a-1)(a+1) \vdots p$, và điều này không thể xảy ra với $2 \leq a \leq p-2$. Vậy thì bằng cách nhóm từng cặp a và $\bar{a}$ ta được

$$2.3.(p-3)(p-2) \equiv 1 (\mathrm{mod}\ p).$$

Nhân các vế với $(p-1)$ ta có

$$(p-1)! \equiv 1.(p-1) \equiv -1 \pmod{p}.$$

Định lý Wilson nêu lên đặc trưng của số nguyên tố vì đảo lại của nó vẫn đúng.

Định lý 2.1.8. Nếu số nguyên $n > 1$ mà $(n-1)! \equiv -1 \pmod{n}$ thì n là số nguyên tố.

Tập các số nguyên được gọi là hệ thặng dư đầy đủ modulo m nếu mọi số nguyên đều đồng dư modulo m với đúng một số nguyên của hệ.

Dễ dàng thấy rằng: một hệ các số nguyên là thặng dư đầy đủ modulo m khi và chỉ khi hệ này có đúng m số đôi một không đồng dư với nhau modulo m.

Định lý 2.1.9. Nếu các số $r_1, r_2, \ldots, r_m$ là một hệ thặng dư đầy đủ modulo m và a nguyên tố cùng nhau với m thì hệ

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

Cũng là một hệ thặng dư đầy đủ modulo m.

Định lý 2.1.10. Định lý nhỏ Fermat. Nếu p là số nguyên tố và p không là ước của a thì $a^{p-1} \equiv 1 \pmod{p}$.

Chứng minh: Không có số nào trong các số a, 2a, … , $(p-1)a$ là chia hết cho p; vì nếu p là ước của ja thì do $(a,p)=1$ nên p là ước của j vô lý với $1<j\leq p-1$. Mặt khác, dễ dàng thấy rằng $(p-1)$ số a, 2a, … , $(p-1)a$ là đôi một không đồng dư với nhau modulo p; do đó chúng đồng dư modulo p với hệ $1,2,\dots,p-1$.

Vậy $a.2\dots(p-1)a\equiv 1.2.\dots(p-1)\ (\mathrm{mod}\ p)$.

Suy ra:

$$a^{p-1}(p-1)!\equiv(p-1)!\ \ (\mathrm{mod}\ p).$$

Vì $\big((p-1)!,p\big)=1$, nên theo định lý 2.1.3 ta có : $a^{p-1}\equiv 1\ (\mathrm{mod}\ p)$.

Nhận xét :

1. Định lý nhỏ Fermat nói rằng nếu n là số nguyên tố và b là số nguyên bất kì thì $b^n\equiv b\ (\mathrm{mod}\ n)$. Điều này cũng có nghĩa là nếu có số nguyên b để $b^n\not\equiv b\ \ (\mathrm{mod}\ n)$. Thì n hợp số hoặc n = 1.

2. Nếu b là một số nguyên dương, n là hợp số và $b^n\equiv b\ (\mathrm{mod}\ n)$. Thì ta nói n là số nguyên tố cơ sở b.

Đối với mỗi số nguyên dương n, chúng ta kí hiệu $\varphi(n)$ là các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n. Hàm số $\varphi(n)$ được gọi là hàm phi – hàm Euler.

Tập gồm $\varphi(m)$ các số nguyên được gọi là hệ thặng dư thu gọn modulo m nếu mọi số nguyên tố cùng nhau với m đều đồng dư đúng một số nguyên của hệ.

Dễ ràng thấy rằng: một hệ các số nguyên là một hệ thặng dư thu gọn modulo m khi và chỉ khi hệ này có đúng $\varphi(m)$ số nguyên tố cùng nhau với m và đôi một không đồng dư với nhau modulo m.

Định lý 2.1.11. Nếu các số $r_1,r_2,\dots,r_{\varphi(m)}$ là một hệ thặng dư thu gọn modulo m và a nguyên tố cùng nhau với m thì hệ

$$ar_1,ar_2,\dots,ar_{\varphi(m)}$$

Cũng là một hệ thặng dư thu gọn modulo m.

Định lý sau đây là một mở rộng của định lý Fermat

Định lý 2.1.12. Định lý Euler. Nếu m là số nguyên dương và $(a, m) = 1$ thì $a^{\varphi(m)} \equiv 1 \pmod m$.

Nếu $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ với p_i là số nguyên tố, $a_i \in \mathbb{N}^*$, i = 1, 2, …, k thì $\varphi(m)$ được tính bằng công thức $\varphi(m) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots (1 - \frac{1}{p_k})$. Với p là số nguyên tố thì $\varphi(p) = p\left(1 - \frac{1}{p}\right) = p - 1, \varphi(p^2) = p(p-1)$

Chứng minh: Lấy hệ thặng dư thu gọn $ar_1, ar_2, \dots, ar_{\varphi(m)}$. Do $(a, m) = 1$. Nên từ định lý trên ta có $ar_1, ar_2, \dots, ar_{\varphi(m)}$ cũng là hệ thặng dư thu gọn. Vậy các số của hệ đồng dư modulo m với các số của hệ kia . Vậy

$$ar_1, ar_2, \dots, ar_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod m$$

Hay $a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod m$

Vì $r_1 r_2 \dots r_{\varphi(m)}, m = 1$ ta suy ra $a^{\varphi(m)} \equiv 1 \pmod m$.

Định lý Euler có rất nhiều ứng dụng. Chẳng hạn, ta có thể dễ dàng xác định nghịch đảo $\bar{a}$ của số nguyên a modulo m, ta đã biết rằng số nguyên a có nghịch đảo modulo m khi chỉ và khi $(a, m) = 1$. Do định lý Euler $a.a^{\varphi(m)-1} = a^{\varphi(m)} \equiv 1 \pmod m$, ta có $\bar{a} = a^{\varphi(m)-1}$.

2.2. Bài toán về sự chia hết.

Bài 2.1. Cho a, b là các số tự nhiên lẻ, p là số nguyên tố lẻ sao cho a + b chia hết cho p và a - b chia hết cho p − 1. Chứng minh rằng $a^b + b^a$ chia hết cho 2p và $a^a + b^b$ chia hết cho 2p.

Lời giải:

Không mất tính tổng quát, giả sử a ≥ b.

Nếu a ⋮ p, b ⋮ p thì hiển nhiên ta có điều phải chứng minh.

Nếu a và b không chia hết p thì ta có $a^b + b^a = (a^b + b^b) + b^b(b^{a-b}-1)$.

Vì b lẻ nên $a^b + b^b$ ⋮.a + b ⋮ p. Áp dụng Định lý Fermat nhỏ thì

$$b^{p-1} - 1 \equiv 0 \pmod p.$$

Mà a − b ⋮ p – 1 nên $b^{a-b} - 1 ⋮ b^{p-1} - 1$. Do đó $b^{a-b} - 1$ ⋮ p .

Mà a, b là các số nguyên lẻ nên $a^b + b^a$ chia hết cho 2.

Vậy $a^b + b^a$ chia hết cho 2p.

Hoàn toàn tương tự thì $a^a + b^b = (b^b + a^b) + a^b(a^{a-b}-1)$ cũng chia hết cho 2p.

Bài 2.2. Tồn tại hay không số nguyên x thỏa mãn $x^{2401} + x^2 + 1$ chia hết cho 2013

Lời giải:

Vì $x^{2401} + x^2 + 1$ chia hết cho 2013 nên $x^{2401} + x^2 + 1$ chia hết cho 11.

Ta có: $x^{2401} + x^2 + 1 = x(x^{2400} - 1) + x^2 + x + 1$

Mà $x(x^{2400} - 1) = x[(x^{10})^{240} - 1^{240}]$ ⋮ $x(x^{10} - 1)$. Áp dụng định lí Fermat nhỏ ta được

$x(x^{10} - 1) \equiv 0 \pmod{11}$ nên $x(x^{2400} - 1)$ chia hết cho 11

Do đó $x^2 + x + 1$ chia hết cho 11

Cho x chạy trên hệ thặng dư đầy đủ modulo 11 ta thấy $x^2 + x + 1$ không chia hết cho 11.

Vậy không tồn tại số nguyên x thỏa mãn đề bài

Bài 2.3. Chứng minh rằng $A = 3^{2^{4n+1}} + 2^{3^{4n+1}} + 5$ chia hết cho 22, với mọi số tự nhiên n

Lời giải:

Theo định lí Fermat nhỏ ta có $3^{10} \equiv 1 \pmod{11}$, $2^{10} \equiv 1 \pmod{11}$. Ta tìm dư trong phép chia 2^{4n+1} và 3^{4n+1} cho 10

Ta có $2^{4n+1} = 2.16^n \equiv 2 \pmod{10}$ nên $2^{4n+1} = 10q + 2$ $(q \in \mathbb{N})$

$3^{4n+1} = 3.81^n \equiv 3 \pmod{10}$ nên $3^{4n+1} = 10k + 3$ $(k \in \mathbb{N})$

Khi đó $A = 3^{2^{4n+1}} + 2^{3^{4n+1}} + 5 = 3^{10q+2} + 2^{10k+3} + 5 = 9.3^{10q} + 8.2^{10k} + 5 \equiv 0 \pmod{11}$ và $A = 9.3^{10q} + 8.2^{10k} + 5 \equiv 0 \pmod{2}$.

Chính vì thế $A = 3^{2^{4n+1}} + 2^{3^{4n+1}} + 5 \equiv 0 \pmod{11}$ hay A chia hết cho 22.

Bài 2.4. Tìm số dư trong phép chia 2015^{2015} cho 11

Lời giải :

Ta có 2013 ⋮ 11 nên $2015 \equiv 2 \pmod{11}$. Khi đó $2015^{2015} \equiv 2^{2015} \pmod{11}$, mà $2^{10} \equiv 1 \pmod{11}$

Do đó, $2015^{2015} \equiv 2^5.2^{2010} = 2^5.(2^{10})^{201} \equiv 2^5 \equiv 10 \pmod{11}$

Vậy 2015^{2015} chia 11 dư 10.

Bài 2.5. Chứng minh rằng số $2012^{2012} + 2013^{2013} - 2014^{2014}$ chia hết cho 99.

Lời giải :

Ta có $2012 \equiv 5 \pmod{9}$ nên $2012^{2012} \equiv (5)^{2012} \pmod{9}$. Mà $5^6 \equiv 1 \pmod{9}$ nên $5^{2012} = 5^2.(5^6)^{335} \equiv 25 \pmod{9} \equiv 7 \pmod{9}$. Do đó $2012^{2012} \equiv 7 \pmod{9}$

$2013 \equiv 6 \pmod{9}$ nên $2013^{2013} \equiv (6)^{2013} \pmod{9}$. Mà $6^2 \equiv 0 \pmod{9}$ nên $6^{2013} = 6.(6^2)^{1006} \equiv 0 \pmod{9}$. Do đó $2013^{2013} \equiv 0 \pmod{9}$

$2014 \equiv 7 \pmod{9}$ nên $2014^{2014} \equiv (7)^{2014} \pmod{9}$. Mà $7^3 \equiv 1 \pmod{9}$ nên $7^{2014} = 7.(7^3)^{671} \equiv 7 \pmod{9}$. Do đó $2014^{2014} \equiv 7 \pmod{9}$

Từ đó ta có $2012^{2012} + 2013^{2013} - 2014^{2014} \equiv 7 + 0 - 7 \equiv 0 \pmod{9}$ (1)

Mặt khác, $2012 \equiv -1 \pmod{11}$ nên $2012^{2012} \equiv (-1)^{2012} \pmod{11} \equiv 1 \pmod{11}$.

$2013 \equiv 0 \pmod{11}$ nên $2013^{2013} \equiv 0 \pmod{11}$.

$2014 \equiv 1 \pmod{11}$ nên $2014^{2014} \equiv 1 \pmod{11}$.

Từ đó ta được: $2012^{2012} + 2013^{2013} - 2014^{2014} \equiv 1 + 0 - 1 \equiv 0 \pmod{11}$ (2)

Lại có (9, 11) = 1 và 9.11 = 99, kết hợp với (1) và (2) ta có

$2012^{2012} + 2013^{2013} - 2014^{2014}$ chia hết cho 99

Bài 2.6. Cho p là số nguyên tố, a_1, a_2, …,a_n là các số nguyên không chia hết cho p ; p_1, p_2, …, p_n và k_1, k_2, …, k_n là các số tự nhiên. Chứng minh rằng : $p_1a_1^{(p-1)k_1} + p_2a_2^{(p-1)k_2} + \cdots + p_na_n^{(p-1)k_n}$ chia hết cho p khi $p_1 + p_2 + \ldots + p_n$ chia hết cho p. *(Trích tài liệu [5])*

Lời giải:

Ta có a_1, a_2, …,a_n là các số nguyên tố cùng nhau với p nên theo định lí Fecmat ta có:

$a_1^{p-1} \equiv 1 \pmod p$ nên $a_1^{(p-1)k_1} \equiv 1 \pmod p$. Khi đó $p_1a_1^{(p-1)k_1} \equiv p_1 \pmod p$.

$a_2^{p-1} \equiv 1 \pmod p$ nên $a_2^{(p-1)k_2} \equiv 1 \pmod p$. Khi đó $p_2a_2^{(p-1)k_2} \equiv p_2 \pmod p$.

.

.

.

$a_n^{p-1} \equiv 1 \pmod p$ nên $a_n^{(p-1)k_n} \equiv 1 \pmod p$. Khi đó $p_na_n^{(p-1)k_n} \equiv p_n \pmod p$.

Do đó $p_1a_1^{(p-1)k_1} + p_2a_2^{(p-1)k_2} + \cdots + p_na_n^{(p-1)k_n} \equiv p_1 + p_2 + \ldots + p_n \pmod p \equiv 0 \pmod p$

Vậy $p_1a_1^{(p-1)k_1} + p_2a_2^{(p-1)k_2} + \cdots + p_na_n^{(p-1)k_n}$ chia hết cho p khi $p_1 + p_2 + \ldots + p_n$ chia hết cho p.

Bài 2.7. Chứng minh rằng số $333^{555^{777}} + 777^{555^{333}}$ chia hết cho 10.

Lời giải:

Ta có $555 \equiv -1 \pmod 4$ nên $555^{777} \equiv (-1)^{777} \equiv -1 \equiv 3 \pmod 4$,

$555^{333} \equiv -1 \equiv 3 \pmod 4$

Do đó $333^{555^{777}} = 3^{4k+3} \equiv 3^3(3^4)^k \equiv 7 \pmod{10}$

$777^{555^{333}} = 7^{4k+3} \equiv 7^3(7^4)^k \equiv 3 \pmod{10}$

Vậy $333^{555^{777}} + 777^{555^{333}} \equiv 3 + 7 \pmod{10} \equiv 0 \pmod{10}$

Bài 2.8. Cho hai số nguyên dương m, n. Chứng minh rằng nếu mn + 1 chia hết cho 24 thì m + n chia hết cho 24.

Lời giải:

Đặt mn + 1 = 24k, với k là số tự nhiên khác 0 (*). Ta sẽ chứng minh m + n chia hết cho 3 và 8

+ Ta thấy nếu m ≡ 1 (mod 3) và n ≡ 1 (mod 3) thì mn + 1 ≡ 2 (mod 3), không thỏa mãn

Nếu m ≡ -1 (mod 3) và n ≡ -1 (mod 3) thì mn + 1 ≡ 2 (mod 3), không thỏa mãn

Nếu m ≡ -1 (mod 3) và n ≡ 1 (mod 3) thì mn + 1 ≡ 0 (mod 3), thỏa mãn đề bài. Khi đó m + n chia hết cho 3

+ Mặt khác, từ (*) ta có m, n là hai số lẻ.

Xét A = mn + 1 + m + n = (m + 1)(n + 1) và

B = mn + 1 – m – n = (m – 1)(n – 1), ta có AB = $(m^2 – 1)(n^2 – 1)$.

Mà $m^2 – 1$ = (m + 1)(m – 1) chia hết cho 8 (tích hai số chẵn liên tiếp chia hết cho 8) và $n^2 – 1$ cũng chia hết cho 8. Do đó AB chia hết cho 64, suy ra A chia hết cho 8 hoặc B chia hết cho 8, suy ra m + n chia hết cho 8

Hơn nữa 24 = 3.8, và (3, 8) = 1. Vậy m + n chia hết cho 24.

Bài 2.9. Chứng minh rằng $10^3 + 2.10^6 + 3.10^9 + … + 26.10^{78}$ chia hết cho13.

Lời giải:

Ta có 10^3 = 1000 ≡ -1 (mod 13), nên $10^{3k} ≡ (-1)^k$ (mod 13) suy ra $k.10^{3k} ≡ k (-1)^k$ (mod 13), với k = 1, 2, …, 26.

Do đó $10^3 + 2.10^6 + 3.10^9 + … + 26.10^{78}$ ≡ -1 + 2 – 3 + 4 - …- 25 + 26 = 13 ≡ 0 (mod 13).

Vậy $10^3 + 2.10^6 + 3.10^9 + … + 26.10^{78}$ chia hết cho13

Bài 2.10. Với a, b, c là ba số nguyên bất kì, chứng minh rằng:

M = abc$(a^3 – b^3)(b^3 – c^3)(c^3 – a^3)$ chia hết cho 7.

Lời giải:

Ta có x^3 ≡ 0, 1, 6 (mod 7)

+ Nếu ít nhất một trong các số a, b, c chia hết cho 7 thì M chia hết cho 7.

+ Nếu không có số nào trong a, b , c chia hết cho 7 thì $a^3 \equiv 1, 6 \pmod 7$, $b^3 \equiv 1, 6 \pmod 7$, $c^3 \equiv 1, 6 \pmod 7$. Vì có ba số mà chỉ có hai số dư khi chia cho 7 nên tồn tại hai số có cùng số dư khi chia cho 7. Giả sử là a^3 và b^3, khi đó $a^3 - b^3$ chia hết cho 7. Vậy M chia hết cho 7.

Bài 2.11. Cho a, b là hai số nguyên dương thỏa mãn a + 20 và b + 13 cùng chia hết cho 21. Chứng minh rằng $S = 4^a + 9^b + a + b - 10$ chia hết cho 21.

Lời giải:

Ta có a + 20 chia hết cho 21 nên $a + 20 \equiv 0 \pmod 3$ hay $a \equiv 1 \pmod 3$; b + 13 chia hết cho 21 nên $b + 13 \equiv 0 \pmod 3$ hay $b \equiv 2 \pmod 3$. Đặt a = 3k + 1, b = 3q + 2, (k, q ∈ ℕ). Khi đó:

$S = 4^a + 9^b + a + b - 10 \equiv 1 + 0 + 1 + 2 - 10 \equiv 0 \pmod 3$ hay S chia hết cho 3 (1)

Mặt khác, $4^a = 4^{3k+1} = 4.64^k \equiv 4 \pmod 7$, $9^b = 9^{3k+2} \equiv 2^{3k+2} \pmod 7 \equiv 4.8^k \equiv 4 \pmod 7$. Và a + 20 chia hết cho 21 nên $a + 20 \equiv 0 \pmod 7$ hay $a \equiv 1 \pmod 7$, b + 13 chia hết cho 21 nên $b + 13 \equiv 0 \pmod 7$ hay $b \equiv 1 \pmod 7$.

Do đó $S = 4^a + 9^b + a + b - 10 \equiv 4 + 4 + 1 + 1 - 10 \pmod 7$ hay S chia hết cho 7 (2)

Mà 7.3 = 21 và (3, 7) = 1 kết hợp với (1) và (2) ta được S chia hết cho 21.

Bài 2.12. Cho a, b là hai số nguyên thỏa mãn $24a^2 + 1 = b^2$. Chứng minh rằng có một và chỉ một trong hai số đó chia hết cho 5.

Lời giải :

Ta có $24a^2 - b^2 = -1$ không chia hết cho 5 nên a và b không đồng thời chia hết cho 5.

Giả sử a và b cùng không chia hết cho 5. Theo định lí Fecmat thì $a^4 - 1 \equiv 0 \pmod 5$ và $b^4 - 1 \equiv 0 \pmod 5$. Do đó $(a^2 + b^2)(a^2 - b^2) = a^4 - b^4 \equiv 0 \pmod 5$

Nếu $a^2 + b^2 \equiv 0 \pmod 5$ thì $25a^2 + 1 = a^2 + b^2 \equiv 0 \pmod 5$ điều này vô lí.

Do đó $a^2 - b^2 \equiv 0 \pmod 5$. Khi đó $23a^2 + 1 = b^2 - a^2 \equiv 0 \pmod 5$.

Vì (a, 5) = 1 nên $a \equiv \pm 1 \pmod 5$ hoặc $a \equiv \pm 1 \pmod 5$.

Nếu $a \equiv \pm 1$ thì $0 \equiv 23a^2 + 1 = 23(\pm 1)^2 + 1 \equiv -1 \pmod 5$, vô lí

Nếu $a \equiv \pm 2$ thì $0 \equiv 23a^2 + 1 = 23(\pm 2)^2 + 1 \equiv -2 \pmod 5$, vô lí

Chính vì vậy điều giả sử là sai. Vậy trong hai số a, b có một và chỉ một số chia hết cho 5.

Bài 2.13. Cho p là số nguyên tố và a, b là hai số nguyên dương. Chứng minh rằng $ab^p - ba^p$ chia hết cho p.

Lời giải:

Ta có $ab^p - ba^p = ab(b^{p-1} - a^{p-1})$.

Nếu ab chia hết cho p thì $ab^p - ba^p$ chia hết cho p.

Nếu ab không chia hết cho p thì (a, p) = (b, p) = 1. Áp dụng định lí Fecmat ta có $a^{p-1} - 1 \equiv 0 \pmod p$, $b^{p-1} - 1 \equiv 0 \pmod p$. Do đó $b^{p-1} - a^{p-1} \equiv 0 \pmod p$ hay $ab^p - ba^p \equiv 0 \pmod p$.

Vậy $ab^p - ba^p$ chia hết cho p.

Bài 2.14. Chứng minh rằng nếu p là một số nguyên tố thì (p - 2)! – 1 chia hết cho p. Nếu p > 5 thì $(p - 2)! - 1 \neq p^n$, n > 1 .

Lời giải:

Theo định lí Wilson ta có $(p - 1)! \equiv -1 \pmod p \equiv p - 1 \pmod p$, suy ra $(p - 1)(p - 2)! \equiv p - 1 \pmod p$.Mà (p, p - 1) = 1 nên $(p - 2)! \equiv 1 \pmod p$

Vậy (p - 2)! – 1 chia hết cho p.

Với p > 5 , giả sử $(p - 2)! - 1 = p^n$, n là số tự nhiên.

Ta có (p – 2)! chia hết cho p – 1 nên $p^n + 1$ chia hết cho p – 1

Mà $p^n + 1 = (p^n - 1) + 2 \equiv 2 \pmod{p - 1}$. Do đó $2 \equiv 0 \pmod{p - 1}$, vô lí vì p > 5.

Vậy với p > 5 thì (p - 2)! – 1 không là lũy thừa của p.

Bài 2.15. Viết liên tiếp các số 111, 112, 113, …, 887, 888 để được số 111112113…887888, chứng minh rằng số này chia hết cho 1998.

Lời giải:

Gọi A = 111112113…887888.

Ta thấy A chẵn nên A chia hết cho 2.

$A = 111.1000^{777} + 112.1000^{776} + 113.1000^{775} + \ldots + 887.1000 + 888$

Do $1000^k \equiv 1 \pmod 9$, với mọi số tự nhiên k nên

$$A \equiv 111 + 112 + \ldots + 888 \equiv 0 \pmod 9$$

Do đó A chia hết cho 999. Mà (2, 999) = 1 và 1998 = 2. 999.

Vậy A chia hết cho 1998

Bài 2.16. Cho số nguyên dương n, biết 2n + 1 và 3n + 1 là hai số chính phương. Chứng minh rằng n chia hết cho 40.

Lời giải:

Vì 2n + 1 là số chính phương, gọi $m^2 = 2n + 1$, mà 2n + 1 lẻ nên m cũng lẻ: m = 2k + 1. Khi đó $2n + 1 = (2k + 1)^2$, suy ra n = 2k(k + 1), do đó n chẵn.

Lại có 3n + 1 là số chính phương, $3n + 1 = r^2$. Do n chẵn nên r lẻ: r = 2t + 1.

Khi đó $3n + 1 = (2t + 1)^2$, suy ra 3n = 4t(t + 1). Kết hợp với n chẵn ta được n chia hết cho 8

Mặt khác, 5n = 2n + 3n = 4(k(k + 1) + t(t + 1)), suy ra k(k + 1) + t(t + 1) chia hết cho 5, suy ra k và t đều chia hết cho 5, suy ra n chia hết cho 5

Ta có n chia hết cho 5 và 8, (5, 8) = 1, Vậy n chia hết cho 40.

Bài 2.17. Chứng minh rằng với n là số tự nhiên thì

a. $4^{2n+1} + 3^{n+2}$ chia hết cho 13.

b. $6^{2n+1} + 5^{n+2}$ chia hết cho 31.

Lời giải:

a. Vì $4^2 \equiv 3 \pmod{13}$ nên với số tự nhiên n, ta có $4^{2n+1} \equiv 4.3^n \pmod{13}$. Lại có $3^2 \equiv -4 \pmod{13}$ nên $3^{n+2} = 3^2.3^n \equiv -4.3^n \pmod{13}$.

Do đó $4^{2n+1} + 3^{n+2} \equiv 0 \pmod{13}$. Vậy $4^{2n+1} + 3^{n+2}$ chia hết cho 13.

b. Vì $6^2 \equiv 5 \pmod{31}$ nên với số tự nhiên n ta có $6^{2n} \equiv 5^n \pmod{31}$.

Mặt khác $6 \equiv -5^2 \pmod{31}$, nhân vế với vế hai đồng dư thức cuối ta được $6^{2n+1} \equiv -5^{n+2} \pmod{31}$. Chính vì thế ta được $6^{2n+1} + 5^{n+2} \equiv 0 \pmod{31}$.

Vậy $6^{2n+1} + 5^{n+2}$ chia hết cho 31.

Bài 2.18. Cho các số nguyên dương m, n nguyên tố cùng nhau. Chứng minh rằng $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$ *(Trích tài liệu [4])*

Lời giải:

Áp dụng định lí Euler ta có $m^{\varphi(n)} \equiv 1 \pmod{n}$, mà $n^{\varphi(m)} \equiv 0 \pmod{n}$ nên $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{n}$. Đặt $m^{\varphi(n)} + n^{\varphi(m)} = np + 1$ $(p \in \mathbb{N})$

Tương tự ta cũng có $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1(\text{mod } m)$, suy ra $np + 1 \equiv 1 \text{ (mod m)}$ hay $np \equiv 0 \text{ (mod m)}$. Mà (m, n) = 1 nên p phải chia hết cho m hay p = mq ($q \in \mathbb{N}$).

Khi đó $m^{\varphi(n)} + n^{\varphi(m)} = mnq + 1$ hay $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1(\text{mod } mn)$.

Bài 2.19. (Đề nghị cho IMO của Đài Loan, 1999). Xác định tất cả các cặp số nguyên dương (n, p) sao cho p nguyên tố, $n \leq 2p$ và $(p - 1)^n + 1$ chia hết cho n^{p-1}.

(Trích tài liệu [1])

Lời giải:

Dễ dàng nhận thấy cặp (1, p), với p là số nguyên tố và cặp (2, 2) thỏa mãn điều kiện bài toán.

Ta tìm những nghiệm (n, p) với $n \geq 2$ và $p \geq 3$.

Vì p lẻ nên $(p - 1)^n + 1$ lẻ, suy ra n lẻ ($n < 2p$). Gọi q là ước số nguyên tố nhỏ nhất của n. Khi đó q là ước của $(p - 1)^n + 1$, nên $(p - 1)^n \equiv -1 \text{ (mod q)}$ và (q, p) = 1.

Mà (n, q - 1) = 1 dẫn đến sự tồn tại của các số nguyên x, y sao cho xn + y(q - 1) = 1, nên: $p - 1 \equiv (p - 1)^{xn}.(p - 1)^{y(p-1)} \equiv (-1)^x.1^y \equiv -1 \text{ (mod q)}$, vì q – 1 chẵn, n lẻ nên x lẻ.

Điều đó chứng tỏ p chia hết cho q, suy ra p = q hay n chia hết cho p và $n < 2p$, suy ra n = p.

Dẫn tới p^{p-1} là ước của $(p - 1)^p + 1 = p[(p - 1)^{p-1} - (p - 1)^{p-2} + \ldots - (p - 1) + 1] =$

$$= (p^p - C_p^1 p^{p-1} + C_p^2 p^{p-2} - \ldots + C_p^{p-3} p^3 - C_p^{p-2} p^2 + p^2 - 1) + 1 =$$

$$= p^2(p^{p-2} - C_p^1 p^{p-3} + C_p^2 p^{p-4} - \ldots + C_p^{p-3} p - C_p^{p-2} + 1)$$

Do mọi số hạng trong dấu ngoặc đều chia hết cho p trừ số hạng cuối nên ta suy ra $p - 1 \leq 2$. Từ đó ta được p = 3 và n = 3.

Vậy các cặp (n, p) thỏa mãn đề bài là (2, 2), (3, 3) và (1, p) với p là số nguyên tố bất kì.

Bài 2.20. (Nga, 1997). Cho m, n là hai số nguyên dương sao cho $2^n - 1$ chia hết cho $(2^m - 1)^2$. Chứng minh rằng n chia hết cho $m(2^m - 1)$.

(Trích tài liệu [1])

Lời giải:

Ta có $2^n - 1$ chia hết cho $2^m - 1$ nên n chia hết cho m. Đặt n = mk, với k là số nguyên dương. Khi đó:

$$\frac{2^n-1}{2^m-1}=\frac{2^{mk}-1}{2^m-1}=1+2^m+2^{2m}+...+2^{(k-1)m}\equiv\underbrace{1+1+...+1}_{k}\equiv k(\text{mod}\,2^m-1)$$

Mà $2^n - 1$ chia hết cho $(2^m - 1)^2$ nên $\frac{2^n-1}{2^m-1} \equiv 0 \pmod{2^m - 1}$. Do đó $k \equiv 0 \pmod{2^m - 1}$, suy ra mk chia hết cho $m(2^m - 1)$ hay n chia hết cho $m(2^m - 1)$.

2.3. Các bài toán về số chính phương

Bài 2.21. Chứng minh số M = 999 . . . .9800...01 (có n số 9 và n số 0) là số chính phương

Lời giải:

Ta có $M = 999...9.10^{n+2} + 8.10^{n+1} + 1$.

Đặt a = 111...1 (n số 1) ta được $9a + 1 = 999..9 + 1 = 100...0 = 10^n$. Khi đó

$M = 9a.100(9a + 1) + 80(9a + 1) + 1 = 8100a^2 + 900a + 720a + 81 = (90a + 9)^2$

Vậy M là bình phương của số 90a + 9 = 999. . .9 (gồm n + 1 số 9) .

Bài 2.22. Cho hai số nguyên x, y đều là tổng của hai số chính phương. Chứng minh rằng tích x.y cũng là tổng của hai số chính phương.

Lời giải:

Đặt $x = a^2 + b^2$; $y = c^2 + d^2$. Ta có : $x.y = a^2d^2 + b^2c^2 + a^2c^2 + b^2d^2$

$= (ac + bd)^2 + (ad - bc)^2$ là tổng hai số chính phương.

Bài 2.23. Cho $p_1p_2...p_n$ là tích của n số nguyên tố đầu tiên. Chứng tỏ rằng

a. $A = p_1p_2...p_n + 1$ không phải là số chính phương.

b. $B = p_1p_2...p_n - 1$ không phải là số chính phương.

Lời giải:

Giả sử A là số chính phương và $A = k^2$ ($k \in \mathbb{Z}$). Khi đó $p_1p_2...p_n = k^2 - 1$ Nếu k chẵn thì k^2 chẵn nên $k^2 - 1$ lẻ. Trong khi đó $p_1p_2...p_n = 2.p_2p_3...p_n$ là số chẵn nên trường hợp này không xảy ra.

Nếu k lẻ thì $k^2 - 1 = (k - 1)(k + 1)$ chia hết cho 4. Khi đó $p_1p_2...p_n$ chia hết cho 4 hay $p_2p_3...p_n$ chia hết cho 2 (điều này vô lý vì các số nguyên tố lớn hơn 2 đều là số lẻ).

Vậy A không thể là số chính phương .

b. Giả sử B là số chính phương và $B = k^2$ ($k \in \mathbb{Z}$) hay $p_1p_2\ldots p_n = k^2 + 1$ Nếu k chẵn thì k^2 chẵn nên $k^2 + 1$ lẻ vô lí vì $p_1p_2\ldots p_n = 2.p_2p_3\ldots p_n$ là số chẵn. Nếu k lẻ thì đặt $k = 2a + 1$. Khi đó $p_1p_2\ldots p_n = k^2 + 1 = 4a^2 + 4a + 2 = 2(2a^2 + 2a + 1)$ hay $p_2p_3\ldots p_n = 2a^2 + 2a + 1$. Xét phép chia $2a^2 + 2a + 1$ cho 3, ta có:

Với $a \equiv 0 \pmod 3$ hoặc $a \equiv -1 \pmod 3$ thì $2a^2 + 2a + 1 \equiv 1 \pmod 3$

Với $a \equiv 1 \pmod 3$ thì $2a^2 + 2a + 1 \equiv 2 \pmod 3$

Do đó $2a^2 + 2a + 1$ không chia hết cho 3, vô lí vì $p_2p_3\ldots p_n$ chia hết cho 3

Vậy B không là số chính phương.

Bài 2.24. Tìm tất cả các số tự nhiên n sao cho $Q(n) = 3^6 + 3^n$ là số chính phương

Lời giải:

Ta có $Q(n) = 3^6 + 3^n = 3^6(1 + 3^{n-6})$. Để Q(n) là số chính phương thì $(1 + 3^{n-6})$ phải là số chính phương. Giả sử $1 + 3^{n-6} = k^2$ thì $(k - 1)(k + 1) = 3^{n-6}$. Khi đó $k - 1$, $k + 1$ là các lũy thừa của 3.

Đặt $k - 1 = 3^a$, $k + 1 = 3^b$, $a, b \in \mathbb{N}$, khi đó $(k + 1) - (k - 1) = 2$ nên $3^a - 3^b = 2$

$\Leftrightarrow 3^a(3^{b-a} - 1) = 2 \Leftrightarrow \begin{cases} 3^a = 1 \\ 3^{b-a} - 1 = 2 \end{cases}$ hoặc $\begin{cases} 3^{b-a} - 1 = 1 \\ 3^a = 2 \end{cases}$ (hệ này vô nghiệm trên $\mathbb{N}$). Do đó $a = 0$, $b = 1$, suy ra $k = 2$, từ đó $1 + 3^{n-6} = 4$, suy ra $n = 7$.

Vậy với $n = 7$ thì $Q(n) = 3^6 + 3^n$ là số chính phương.

Bài 2.25. Cho dãy số 49, 4489, 444889, … được thành lập bằng cách thêm số 48 vào giữa số đứng trước nó. Chứng minh rằng tất cả các số thuộc dãy trên đều là số chính phương.

(Trích tài liệu [5])

Lời giải:

Số hạng tổng quát của dãy có dạng: $a_n = \underbrace{44\ldots4}_{\text{n số}}\underbrace{88\ldots8}_{\text{n−1 số}} = \underbrace{44\ldots4}_{\text{n số}}\underbrace{88\ldots8}_{\text{n số}} + 1$

$$= \underbrace{44\ldots4}_{\text{n số}}.10^n + \underbrace{88\ldots8}_{\text{n số}} + 1$$

$$= 4.\frac{10^n - 1}{9}.10^n + 8.\frac{10^n - 1}{9} + 1$$

$$= \frac{1}{9}(4.10^{2n} - 4.10^n + 8.10^n - 8 + 9)$$

$= \frac{1}{9}(4.10^{2n} + 4.10^{n} + 1) = (\frac{2.10^{n}+1}{3})^2$

Vì $2.10^n \equiv 2 \pmod 3$ nên $2.10^n + 1 \equiv 0 \pmod 3$. Do đó $\frac{2.10^n+1}{3}$ là số nguyên nên a_n là số chính phương. Vậy tất cả các số của dãy trên đều là số chính phương.

Bài 2.26. Chứng minh rằng nếu hiệu các lập phương của hai số nguyên liên tiếp là bình phương của một số tự nhiên n thì n là tổng của hai số chính phương liên tiếp.

Lời giải:

Gọi hai số nguyên liên tiếp là k và k + 1. Khi đó $n^2 = (k - 1)^3 – k^3 = 3k^2 + 3k + 1$ hay $4n^2 = 12k^2 + 12k + 4 = 3(2k + 1)^2 + 1$, suy ra $(2n + 1)(2n - 1) = 3(2k + 1)^2$

+) Nếu 2n – 1 chia hết cho 3 thì do (2n – 1, 2n + 1) = 1 và $\frac{2n-1}{3}(2n + 1) = (2k + 1)^2$ là số chính phương nên $2n – 1 = 3u^2$ và $2n + 1 = v^2$, với uv = 2k + 1, (u, v) = 1 và v không chia hết cho 3.

Vì v lẻ và không chia hết cho 3 nên v có dạng $6t \pm 1$.

Khi đó $2n + 1 = v^2 = 36t^2 \pm 12t + 1$ và $3u^2 = 2n – 1 = 36t^2 \pm 12t – 2 \equiv 2 \pmod 3$ không phải số chính phương.

+) Nếu 2n + 1 chia hết cho 3 thì do (2n – 1, 2n + 1) = 1 và $\frac{2n+1}{3}(2n - 1) = (2k + 1)^2$ là số chính phương nên $2n – 1 = u^2$ và $2n + 1 = 3v^2$, với uv = 2k + 1, (u, v) = 1 và u không chia hết cho 3.

Vì u lẻ và không chia hết cho 3 nên u có dạng $6s \pm 1$.

Khi đó $2n - 1 = u^2 = 36s^2 \pm 12s + 1$ và $3v^2 = 2n + 1 = 36s^2 \pm 12s + 1$.

Do đó $n = 18s^2 \pm 16s + 1 = (3s)^2 + (3s \pm 1)^2$.

Vậy n là tổng của hai số chính phương liên tiếp.

Bài 2.27. Chứng minh rằng số $A = (10^n + 10^{n-1} + … + 10 + 1)(10^{n+1} + 5) + 1$ là số chính phương.

Lời giải :

Ta có $10^{n+1} – 1 = (10 - 1)(10^n + 10^{n-1} + … + 10 + 1)$ nên

$10^n + 10^{n-1} + … + 10 + 1 = \frac{1}{9}(10^{n+1} - 1)$. Khi đó

$A = \frac{1}{9}(10^{n+1} - 1)(10^{n+1} + 5) + 1 = \frac{1}{9}(10^{2n+2} + 4.10^{n+1} - 5 + 9)$

$= \frac{1}{9}(10^{2n+2} + 4.10^{n+1} + 4) = (\frac{10^{n+1}+2}{3})^2$.

Vậy A là số chính phương.

Bài 2.28. Cho n là số nguyên dương và d là một ước nguyên dương của $3n^2$. Chứng minh rằng $n^2 + d$ là một số chính phương khi và chỉ khi $d = 3n^2$.

Lời giải :

Nếu $n^2 + d$ là một số chính phương, giả sử $3n^2 = dk$ $(k > 0)$.

Khi đó $n^2 + d = n^2 + \frac{3n^2}{k}$ là số chính phương nên $n^2(k^2 + 3k)$ là số chính phương, đặt $k^2 + 3k = m^2$ $(m > 0)$ hay $(2k + 3)^2 - 4m^2 = 9$

$\Leftrightarrow (2k + 3 - 2m)(2k + 3 + 2m) = 9$

Mà $2k + 3 + 2m > 2k + 3 - 2m$ và $2k + 3 + 2m \geq 0$ nên

$$\begin{cases} 2k + 3 + 2m = 9 \\ 2k + 3 - 2m = 1 \end{cases} \Leftrightarrow \begin{cases} k = 1 \\ m = 2 \end{cases}.$$

Do đó $d = 3n^2$

Ngược lại, ta có $d = 3n^2$ thì $n^2 + d = n^2 + 3n^2 = (2n)^2$ là một số chính phương.

Vậy $n^2 + d$ là một số chính phương khi và chỉ khi $d = 3n^2$.

Bài 2.29. Chứng minh rằng không tồn tại số nào trong dãy số vô hạn

$$11, 111, 1111, 11111, \ldots$$

biểu diễn dưới dạng tổng của hai số chính phương.

Lời giải :

Ta thấy $x^2 \equiv 0, 1 \pmod 4$ và $y^2 \equiv 0, 1 \pmod 4$ nên $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$ (1).

Ta sẽ chứng minh $a_n = \underbrace{11...11}_{\text{n chữ số 1}} \equiv 3 \pmod 4$, với mọi $n \geq 2$

Thật vậy, với $n = 2$, $a_2 = 11 \equiv 3 \pmod 4$.

Giả sử $a_k \equiv 3 \pmod 4$, đặt $a_k = 4t + 3$ ($t \geq 2$). Khi đó $a_{k+1} = 10a_n + 1 = 10(4t + 3) + 1 = 40t + 31 \equiv 3 \pmod 4$. Suy ra $a_n \equiv 3 \pmod 4$ với $n \geq 2$. Kết hợp với (1) ta có được a_n không thể là tổng của hai số chính phương.

Bài 2.30. Chứng minh rằng nếu n có dạng $n = 4^m(8k + 7)$ với $m, k \in \mathbb{N}$ thì n không biểu diễn được thành tổng của ba số chính phương.

Lời giải:

Giả sử ngược lại, $n = 4^m(8k + 7) = x^2 + y^2 + z^2$.

Ta có $x^2 \equiv a \in \{0; 1; 4\} \pmod 8$. Khi đó $n = x^2 + y^2 + z^2 \equiv a \in \{0; 1; 2; 3; 4; 5; 6\} \pmod 8$ (*).

Nếu $m = 0$ thì $n = 8k + 7 \equiv 7 \pmod 8$, mâu thuẫn với (*).

Nếu $m > 0$ thì $n \equiv 0 \pmod 4$, do đó $x^2 + y^2 + z^2 \equiv a \in \{0;4\} \pmod 8$,

$x^2 + y^2 + z^2 \equiv 0 \pmod 4$. Vì $x^2 \equiv a \in \{0;1\} \pmod 4$ nên $x^2 \equiv y^2 \equiv z^2 \equiv 0 \pmod 4$.

Do đó $x = 2x_1$; $y = 2y_1$; $z = 2z_1$ và $x_1^2 + y_1^2 + z_1^2 \equiv 4^{m-1}(8k+7)$. Tiếp tục như vậy sẽ dẫn đến $x_m^2 + y_m^2 + z_m^2 = 8k + 7 \equiv 7 \pmod 8$, mâu thuẫn với (*).

Vậy nếu n có dạng $n = 4^m(8k + 7)$ với $m, k \in \mathbb{N}$ thì n không biểu diễn được thành tổng của ba số chính phương.

Bài 2.31. (Đề tuyển sinh THPT chuyên ĐHSP Hà Nội - 2014). Chứng minh rằng với mỗi số nguyên $n \geq 6$ thì số:

$a_n = 1 + \dfrac{2.6.10...(4n-2)}{(n+5)(n+6)...(2n)}$ là một số chính phương.

(Trích tài liệu [2])

Lời giải :

Ta có $a_n = 1 + \frac{2.6.10...(4n-2)}{(n+5)(n+6)...(2n)} = 1 + \frac{2^n(1.3.5...(2n-1))(n+4)!}{(2n)!} = 1 + \frac{2^n(n+4)!}{2.4.6...2n}$

$= 1 + \frac{2^n.1.2.3..n(n+1)(n+2)(n+3)(n+4)}{2^n.1.2.3...n} = 1 + (n+1)(n+2)(n+3)(n+4)$

$= 1 + n^4 + 10n^3 + 35n^2 + 50n + 24 = (n^2 + 5n + 5)^2$

Vậy a_n là một số chính phương.

Bài 2.32. (Đề tuyển sinh THPT chuyên Hà Nam, 2013 - 2014). Cho số nguyên dương n và các số $A = \underbrace{444...4}_{2n \text{ chữ số } 4}$, $B = \underbrace{888...8}_{n \text{ chữ số } 8}$.

Chứng minh rằng A + 2B + 4 là số chính phương.

(Trích tài liệu [2])

Lời giải :

Ta có :

$$A = \underbrace{444...4}_{2n \text{ chữ số } 4} = \underbrace{444...4}_{n \text{ chữ số } 4}\underbrace{000...0}_{n \text{ chữ số } 0} + \underbrace{444...4}_{n \text{ chữ số } 4} = \underbrace{444...4}_{n \text{ chữ số } 4}(10^n - 1) + \underbrace{888...8}_{n \text{ chữ số } 8}$$

$$= 4.\underbrace{111...1}_{n \text{ chữ số } 1}.\underbrace{999...9}_{n \text{ chữ số } 9} + B = 4.\underbrace{111...1}_{n \text{ chữ số } 1}.9.\underbrace{111...1}_{n \text{ chữ số } 1} + B = (6.\underbrace{111...1}_{n \text{ chữ số } 1})^2 + B$$

$$= (\frac{3}{4}.\underbrace{888...8}_{n \text{ chữ số } 8})^2 + B = (\frac{3}{4}B)^2 + B$$

Khi đó $A + 2B + 4 = \left(\frac{3}{4}B\right)^2 + B + 2B + 4 = \left(\frac{3}{4}B\right)^2 + 2.\frac{3}{4}B.2 + 4 = \left(\frac{3}{4}B + 2\right)^2$

$$= \left(\frac{3}{4}.\underbrace{888...8}_{n \text{ chữ số } 8} + 2\right)^2 = \left(3.\underbrace{222...2}_{n \text{ chữ số } 2} + 2\right)^2 = \left(\underbrace{666...6}_{n-1 \text{ chữ số } 6}8\right)^2$$

Vậy A + 2B + 4 là số chính phương.

Bài 2.33. (Malaysia, 2000) Chứng minh rằng $2^{2p} + 2^{2q}$ không phải số chính phương, với p, q là các số nguyên không âm.

(Trích tài liệu [1])

Lời giải:

Không mất tính tổng quát ta giả sử $p \geq q$, ta có:

$$2^{2p} + 2^{2q} = 4^q(4^{p-q} + 1)$$

Vì 4^q là số chính phương nên ta cần chứng minh $4^{p-q} + 1$ không phải số chính phương.

Giả sử ngược lại, tức là tồn tại số nguyên n sao cho $4^{p-q} + 1 = (2n + 1)^2$, thì $4^{p-q} + 1 = 4n^2 + 4n + 1$, suy ra $4^{p-q-1} = n(n + 1)$, vô lí vì một trong hai số n hoặc n + 1 là số lẻ. Do đó điều giả sử là sai, $4^{p-q} + 1$ không phải số chính phương.

Vậy $2^{2p} + 2^{2q}$ không phải số chính phương, với p, q là các số nguyên không âm.

2.4. Các bài toán về chữ số tận cùng.

Một số tính chất áp dụng :

Với số tự nhiên $k > 0$, ta có :

+ Nếu $a \equiv 0 \pmod{10}$ thì $a^{20k} \equiv 00 \pmod{100}$ và $a^{100k} \equiv 000 \pmod{1000}$

+ Nếu $a \equiv 1, 3, 7, 9 \pmod{10}$ thì $a^{20k} \equiv 01 \pmod{100}$ và $a^{100k} \equiv 001 \pmod{1000}$

+ Nếu $a \equiv 5 \pmod{10}$ thì $a^{20k} \equiv 25 \pmod{100}$ và $a^{100k} \equiv 625 \pmod{1000}$

+ Nếu $a \equiv 2, 4, 6, 8 \pmod{10}$ thì $a^{20k} \equiv 76 \pmod{100}$ và $a^{100k} \equiv 376 \pmod{1000}$

Bài 2.34. Tìm chữ số tận cùng của số $A = 7^{2016^{2015}} - 3^{216^{215}}$.

Lời giải :

Ta có $7^4 \equiv 1 \pmod{10}$ nên với số tự nhiên m thì $7^{4m} \equiv 1 \pmod{10}$. Mà $2016^{2015} = (4.504)^{2015} = 4.4^{2014}.504^{2015}$. Do đó $7^{2016^{2015}} = 7^{4(4^{2014}.504^{2015})} \equiv 1 \pmod{10}$

Mặt khác, $3^4 \equiv 1 \pmod{10}$ nên với số tự nhiên 2 thì $3^{4n} \equiv 1 \pmod{10}$.

Mà $216^{215} = (4.54)^{215} = 4.4^{214}.54^{215}$. Do đó $3^{216^{215}} = 3^{4(4^{214}.54^{215})} \equiv 1 \pmod{10}$.

Từ đó ta được $7^{2016^{2015}} - 3^{216^{215}} \equiv 0 \pmod{10}$.

Vậy chữ số tận cùng của $7^{2016^{2015}} - 3^{216^{215}}$ là số 0.

Bài 2.35. Tìm chữ số tận cùng của số $B = 1 + 3^{1992} + 5^{1994} + 7^{1996} + 9^{1998}$.

(Trích tài liệu [6])

Lời giải :

Ta có $3^4 \equiv 1 \pmod{10}$ nên $3^{1992} = (3^4)^{498} \equiv 1 \pmod{10}$.

$5^n \equiv 5 \pmod{10}$ nên $5^{1994} \equiv 5 \pmod{10}$

$7^4 \equiv 1 \pmod{10}$ nên $7^{1996} = (7^4)^{499} \equiv 1 \pmod{10}$

$9^2 \equiv 1 \pmod{10}$ nên $9^{1998} = (9^2)^{999} \equiv 1 \pmod{10}$

Do đó $1 + 3^{1992} + 5^{1994} + 7^{1996} + 9^{1998} \equiv 1 + 1 + 5 + 1 + 1 \equiv 9 \pmod{10}$

Vậy chữ số tận cùng của B là số 9.

Bài 2.36. Tìm hai chữ số tận cùng của số $C = 7^{2^{4n+1}} + 4^{3^{4n+1}} - 65$.

Lời giải :

Ta có $7^4 = 2401 \equiv 0 \pmod{100}$ và $4^{10} \equiv 76 \pmod{100}$ nên

$7^{2^{4n+1}} = 7^{2.2^{4n}} = 7^{4m} \equiv 1 \pmod{100}$,

$4^{3^{4n+1}} = 4^{3.81^n} = 4^{10n+3} = 4^3(4^{10})^n \equiv 64.76^n \equiv 64.76 \equiv 64 \pmod{100}$

Do đó C = $7^{2^{4n+1}} + 4^{3^{4n+1}} - 65 \equiv 11 + 64 - 65 \pmod{100}$

Vậy hai chữ số tận cùng của số C là số 00.

Bài 2.37. Tìm ba chữ số tận cùng của số $2^{9^{2003}}$

Lời giải:

Ta tìm hai chữ số tận cùng của 9^{2003}. Ta có $9^{2003} = 9^3.9^{2000} = 9^3(3^{20})^{200} \equiv 29 \pmod{100}$.

Do đó $2^{9^{2003}} = 2^{100k+29} = 2^{29}.(2^{100})^k \equiv 912.376 \equiv 912 \pmod{1000}$.

Vậy ba chữ số tận cùng của $2^{9^{2003}}$ là số 912.

Bài 2.38. Tìm chữ số tận cùng của số $\left[\frac{10^{2000}}{10^{100}+3}\right]$

(Trích tài liệu [5])

Lời giải:

Ta có $\frac{10^{2000}}{10^{100}+3} = \frac{10^{2000}-3^{20}}{10^{100}+3} + \frac{3^{20}}{10^{100}+3}$

Khi đó $3^{20} < 9^{10} < 10^{10} < 10^{100} + 3$ nên ta có $0 < \frac{3^{20}}{10^{100}+3} < 1$.

và $10^{2000} - 3^{20} \vdots 10^{200} - 3^2 \vdots 10^{100} + 3$.

Do đó $\left[\frac{10^{2000}}{10^{100}+3}\right] = \frac{10^{200}-3^{20}}{10^{100}+3}(10^{200.9} + 10^{200.8}.3^2 + ... + 10^{200.1}.3^{2.8} + 3^{2.9})$

$= (10^{100} - 3)(10^{1800} + 10^{1600}.3^2 + \ldots + 10^{200}.3^{16} + 3^{18})$

Mà $10^{100} - 3 \equiv -3 \pmod{10}$

$10^{1800} + 10^{1600}.3^2 + \ldots + 10^{200}.3^{16} + 3^{18} \equiv 3^{18} = 3^{4.4+2} = 9.81^4 \equiv 9 \pmod{10}$

Nên $\left[\frac{10^{2000}}{10^{100}+3}\right] \equiv -3.9 \equiv -27 \equiv 3 \pmod{10}$

Vậy chữ số tận cùng của $\left[\frac{10^{2000}}{10^{100}+3}\right]$ là số 3.

Bài 2.39. Tìm hai chữ số tận cùng của số 8888^{8888}.

Lời giải:

Ta có $8888 \equiv 88 \pmod{100}$ nên $8888^{8888} \equiv 88^{8888} \pmod{100}$.

Mà $88^{8888} \equiv 0 \pmod 4$ (1). Và (44, 25) = 1 nên theo định lí Euler ta có $88^{\varphi(25)} \equiv 1 \pmod{25}$ hay $88^{20} \equiv 1 \pmod{25}$, do đó $88^{8880} = (88^{20})^{444} \equiv 1 \pmod{25}$.

Lại có $88 \equiv 13 \pmod{25}$, nên $88^2 \equiv -6 \pmod{25}$, suy ra $88^8 \equiv (-6)^4 \equiv -4 \pmod{25}$.

Từ đó ta được $88^{8888} \equiv -4 \pmod{25}$ (2)

Từ (1) và (2) có $88^{8888} \equiv 0 \pmod 4 \equiv 96 \pmod 4$ và $88^{8888} \equiv -4 \pmod{25} \equiv 96 \pmod{25}$. Do đó $8888^{8888} \equiv 88^{8888} \pmod{100} \equiv 96 \pmod{100}$.

Vậy hai chữ số tận cùng của 8888^{8888} là 96.

Bài 2.40. Tìm hai chữ số tận cùng của $S = 1^{2002} + 2^{2002} + \ldots + 2004^{2002}$

Lời giải:

Ta có: Với a là số tự nhiên, nếu a chẵn thì a^2 chia hết cho 4, nếu a lẻ thì $a^{100} - 1$ chia hết cho 4. Nếu a chia hết cho 5 thì a^2 chia hết cho 25, nếu a không chia hết cho 5 thì (a, 25) = 1, theo định lí Euler thì $a^{\varphi(25)} \equiv 1 \pmod{25}$ hay $a^{20} \equiv 1 \pmod{25}$, suy ra $a^{100} \equiv 1 \pmod{25}$ hay $a^{100} - 1$ chia hết cho 25.

Do đó với số tự nhiên a ta có $a^2(a^{100} - 1)$ chia hết cho 100. Khi đó

$S = 1^{2002} + 2^{2002} + \ldots + 2004^{2002}$

$= 1^{2002} + 2^2(2^{2000} - 1) + \ldots + 2004^2(2004^{2000} - 1) + 2^2 + 3^2 + \ldots + 2004^2$

$\equiv 1^2 + 2^2 + 3^2 + \ldots + 2004^2 \pmod{100}$

Áp dụng công thức $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ ta có

$1^2 + 2^2 + 3^2 + \ldots + 2004^2 = \frac{2004.2005.4009}{6} = 334.2005.4009 = 2684707030$

Vậy $S \equiv 1^2 + 2^2 + 3^2 + \ldots + 2004^2 \pmod{100} \equiv 30 \pmod{100}$ hay hai chữ số tận cùng của S là 30.

Bài 2.41. (Olympic 30 – 4 - 2014)). Cho hai số tự nhiên m và n sao cho $m > n \geq 1$. Biết rằng hai chữ số tận cùng của 2014^m bằng với hai chữ số tận cùng của 2014^n theo cùng thứ tự. Tìm các số m, n sao cho m + n có giá trị nhỏ nhất.

(Trích tài liệu [1])

Lời giải:

Vì $m > n \geq 1$ nên 2014^m và 2014^n có hai chữ số tận cùng bằng nhau theo đúng thứ tự thì

$2014^m - 2014^n = 2014^n(2014^{m-n} - 1)$ chia hết cho 100 (1)

Do 2014^{m-n} lẻ, kết hợp với (1) ta có 2014^n chia hết cho 4, suy ra $n \geq 2$ và $(2014^{m-n} - 1)$ chia hết cho 25. (2)

Đặt $m - n = 10k + r$ với k, r là các số tự nhiên, $0 \leq r \leq 9$. Khi đó

$2014^{m-n} \equiv 14^{m-n} = (14^5)^{2k}.14^r = (537824^2)^k.14^r \equiv ((-1)^2)^k.14^r \equiv 14^r \pmod{25}$. Kết hợp với (2) ta được $14^r \equiv 1 \pmod{25}$, với $0 \leq r \leq 9$. Thay các giá trị của r ta thấy chỉ có r = 0 là thỏa mãn.

Do đó $m = 10k + n$. Mà $m > n$ nên $k \geq 1$. Lại có $n \geq 2$ nên

$$m + n = 2n + 10k \geq 2.2 + 10.1 = 14$$

Dấu " = " xảy ra khi $k = 1$ và $n = 2$, suy ra $m = 12$.

Vậy với $m = 12$ và $n = 2$ thì $m + n$ đạt giá trị nhỏ nhất.

2.5. Phương trình nghiệm nguyên.

2.5.1. Phương pháp đồng dư, chia hết

Bài 2.42. Chứng minh rằng phương trình sau không có nghiệm nguyên :

$$x^{30} + y^{30} + z^{30} = 37^{2015} + 27^{2015} + 16^{2015}.$$

Lời giải :

Ta có $37^{2015} = (4.9 + 1)^{2015}$, suy ra $37^{2015} \equiv 1 \pmod 9$

$27^{2015} \equiv 0 \pmod 9$

$16^{2015} = (2.9 - 2)^{2015} \equiv (-2)^{2015} \pmod 9 \equiv -4.2^{2013} \pmod 9 \equiv -4.(2^3)^{671} \pmod 9$. Mà $2^3 \equiv -1 \pmod 9$ nên $(2^3)^{671} \equiv -1 \pmod 9$.

Do đó $16^{2015} \equiv -4.(-1) \pmod 9 \equiv 4 \pmod 9$

Vậy $37^{2015} + 27^{2015} + 16^{2015} \equiv 5 \pmod 9$.

Mặt khác, lập phương của một số tự nhiên khi chia cho 9 chỉ có thể cho các số dư là -1, 0 hoặc 1 nên ta có

$x^{30} + y^{30} + z^{30} = (x^{10})^3 + (y^{10})^3 + (z^{10})^3$ khi chia cho 9 có các số dư là -3, -1, 0, 1, 3

Vì vậy hai vế của phương trình đã cho không có cùng số dư khi chia cho 9 nên phương trình không có nghiệm nguyên.

Bài 2.43. Giải phương trình nghiệm nguyên không âm : $3^x + 1 = 2^y$

Lời giải :

+ Xét $y = 0$, được $3^x + 1 = 1$(vô nghiệm)

+ Xét y = 1, được $3^x + 1 = 2$, suy ra x = 0.

+ Xét y = 2, được $3^x + 1 = 4$, suy ra x = 1

+ Xét y > 2 có 2^y chia hết cho 8

Ta xét số dư của $3^x + 1$ chia cho 8.

Với x = 0, 1 thì $3^x + 1$ không chia hết cho 8

Với x > 1, xét x chẵn có 3^x chia 8 dư 1 nên $3^x + 1$ chia 8 dư 2.

x lẻ thì 3^x chia 8 dư 3 nên $3^x + 1$ chia 8 dư 4.

Do đó với y > 2 thì phương trình đã cho không có nghiệm nguyên.

Vậy phương trình có nghiệm là (0, 1) và (1, 2)

Bài 2.44. (Đề tuyển sinh THPT trường KHTN – ĐHQGHN, 2005). Tìm nghiệm nguyên của phương trình $x^2 + 17y^2 + 34xy + 51(x + y) = 1740$

(Trích tài liệu [2])

Lời giải:

Ta có : $x^2 + 17y^2 + 34xy + 51(x + y) = 1740$

$\Leftrightarrow x^2 + 17[y^2 + 2xy + 3(x + y)] = 1740$

Ta thấy rằng với mọi số nguyên x, x có thể có dạng sau :

$x = 17k \pm r$ với r = 0, 1, 2, 3, 4, 5, 6, 7, 8.

Từ đó suy ra x^2 có các dạng tương ứng sau :

$x^2 = 17k, 17k + 1, 17k + 4, 17k + 9, 17k + 16, 17k + 8, 17k + 2, 17k + 15, 17k + 13$

Do đó vế trái khi chia cho 7, trong mọi tường hợp đều không có số dư là 6. mà vế phải 1740 khi chia cho 17 có số dư là 6.

Vậy phương trình đã cho không có nghiệm nguyên.

2.5.2. Phương pháp phân tích

Bài 2.45. Giải phương trình nghiệm nguyên dương sau:

$$3x^2 + 2y^2 + z^2 + 4xy + 2yz = 26 - 2xz$$

Lời giải:

$$3x^2 + 2y^2 + z^2 + 4xy + 2yz = 26 - 2xz$$

$$\Leftrightarrow x^2 + (x^2 + 2xy + y^2) + (x^2 + y^2 + z^2 + 2xy + 2yz + 2zx) = 26$$

$$\Leftrightarrow x^2 + (x + y)^2 + (x + y + z)^2 = 26$$

$$\Leftrightarrow x^2 + (x + y)^2 + (x + y + z)^2 = 1^2 + 3^2 + 4^2.$$

Do x, y, z là các số nguyên dương nên $x < x + y < x + y + z$. Vì vậy

$$\begin{cases} x = 1 \\ x + y = 3 \\ x + y + z = 4 \end{cases} \Leftrightarrow \begin{cases} x = 1 \\ y = 2 \\ z = 1 \end{cases}$$

Vậy phương trình có nghiệm (1, 2, 1).

Bài 2.46. Giải phương trình nghiệm nguyên : $x^2 - 2^y = 33$.

Lời giải :

+ Xét y chẵn: đặt y = 2k, với k là số tự nhiên, ta được phương trình :

$(x - 2^k)(x + 2^k) = 33$

$$\Leftrightarrow \begin{cases} x - 2^k = 1 \\ x + 2^k = 33 \end{cases} \text{ hoặc } \begin{cases} x - 2^k = 33 \\ x + 2^k = 1 \end{cases} \text{ hoặc } \begin{cases} x - 2^k = -33 \\ x + 2^k = -1 \end{cases} \text{ hoặc } \begin{cases} x - 2^k = -1 \\ x + 2^k = -33 \end{cases}$$

Từ đó ta được k = 4, x = 17 và y = 8.

+ Với y lẻ : đặt y = 2k + 1 ta được phương trình : $x^2 = 33 + 2.2^{2k}$ (*)

Xét số dư khi chia hai vế phương trình (*) cho 3 : ta có $33 + 2.2^{2k}$ chia 3 dư 2 trong khi x^2 chia 3 chỉ có thể có số dư là 0 hoặc 1. Do đó phương trình (*) vô nghiệm.

Vậy phương trình đã cho có nghiệm (17, 8)

Bài 2.47. (Đề tuyển sinh THPT trường KHTN – ĐHQGHN, 2003). Tìm nghiệm nguyên của phương trình $2y^2x + x + y + 1 = x^2 + 2y^2 + xy$

(Trích tài liệu [2])

Lời giải :

Ta có $2y^2x + x + y + 1 = x^2 + 2y^2 + xy$

$\Leftrightarrow 2y^2(x – 1) – x (x - 1) – y(x - 1) = -1$

$\Leftrightarrow (2y^2 – x - y)(x - 1) = -1$

$$\Leftrightarrow \begin{cases} 2y^2 - x - y = -1 \\ x - 1 = 1 \end{cases} hoặc \begin{cases} 2y^2 - x - y = 1 \\ x - 1 = -1 \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 2 \\ y = 1 \end{cases} hoặc \begin{cases} x = 0 \\ y = 1 \end{cases}$$

Vậy phương trình đã cho có nghiệm (0, 1), (2, 1).

2.5.3. Phương pháp đánh giá

Bài 2.48. Tìm nghiệm nguyên dương của phương trình :

$$5(x + y + z + t) + 10 = 2xyzt$$

Lời giải :

Do vai trò của x, y, z, t như nhau nên không mất tính tổng quát, giả sử

$x \geq y \geq z \geq t \geq 1$

Vì x, y, z, t khác 0 nên chia cả hai vế phương trình cho xyzt ta được :

$2 = \frac{5}{yzt} + \frac{5}{xzt} + \frac{5}{xyt} + \frac{5}{xyz} + \frac{10}{xyzt} \leq \frac{30}{t^3}$, suy ra $t^3 \leq 15$, suy ra t = 1 hoặc t = 2.

+ Với t = 1 ta có 5(x + y + z) + 15 = 2xyz. Chia cả hai vế cho xyz ta được

$2 = \frac{5}{yz} + \frac{5}{xz} + \frac{5}{xy} + \frac{15}{xyz} \leq \frac{30}{z^2}$, suy ra $z^2 \leq 15$, suy ra z = 1, z = 2, hoặc z = 3

Với z = 1 thì $5(x + y) + 20 = 2xy \Leftrightarrow (2x - 5)(2y - 5) = 65$. Giải phương trình ước số này ta được các nghiệm (35, 3) và (9, 5). Do đó nghiệm của phương trình đã cho là (35, 3, 1, 1) và (9, 5, 1, 1) và các hoán vị của chúng.

Với z = 2, 3 thì phương trình không có nghiệm nguyên dương.

+ Với t = 2 ta có $5(x + y + z) + 20 = 4xyz$. Chia cả hai vế cho xyz ta được

$4 = \frac{5}{yz} + \frac{5}{xz} + \frac{5}{xy} + \frac{20}{xyz} \leq \frac{35}{z^2}$, suy ra $z^2 \leq \frac{35}{4}$, suy ra z = 2. Khi đó

$5(x + y) + 30 = 8xy \Leftrightarrow (8x - 5)(8y - 5) = 265$.

Do $x \geq y \geq z \geq 2$ nên $8x - 5 \geq 8y - 5 \geq 11$. Mà 265 = 53.5. Suy ra phương trình không có nghiệm nguyên dương.

Vậy phương trình đã cho có nghiệm là (35, 3, 1, 1) và (9, 5, 1, 1) và các hoán vị của chúng.

Bài 2.49 (Đề tuyển sinh THPT trường KHTN – ĐHQGHN, 2006). Tìm nghiệm nguyên của phương trình $8x^2y^2 + x^2 + y^2 = 10xy$

(Trích tài liệu [2])

Lời giải:

Ta thấy x = 0, y = 0 là nghiệm của phương trình

Nếu x, y đều khác 0, áp dụng bất đẳng thức AM-GM, ta có $x^2 + y^2 \geq 2xy$. Khi đó

$8x^2y^2 + x^2 + y^2 \geq 8x^2y^2 + 2xy$, hay $10xy \geq 8x^2y^2 + 2xy$.

Suy ra $8xy \geq 8x^2y^2$ hay $xy \geq x^2y^2$. Do đó $0 < xy \leq 1$, ta tìm được x = y = 1 hoặc x = y = -1.

Vậy nghiệm của phương trình là (0, 0), (1, 1), (-1, -1)

Bài 2.50. (Đề tuyển sinh THPT HN – Amsterdam, 2006). Giải phương trình nghiệm nguyên dương $(y + 1)^4 + y^4 = (x + 1)^2 + x^2$

(Trích tài liệu [2])

Lời giải:

Ta có $2y^4 < y^4 + (y + 1)^4 = (x + 1)^2 + x^2 < 2(x + 1)^2$, suy ra $y < x + 1$. (1)

Mặt khác, $2x^2 < (x + 1)^2 + x^2 = y^4 + (y + 1)^4 < 2(y + 1)^4$, suy ra $x < y + 1$ hay $x - 1 < y$. (2)

Từ (1) và (2) ta có $x - 1 < y < x + 1$. Do x, y nguyên dương nên $x = y$. Khi đó ta được phương trình $(x + 1)^4 + x^4 = (x + 1)^2 + x^2$ có nghiệm $x = 0$

Vậy phương trình đã cho có nghiệm (0, 0)

2.5.4. Phương pháp xuống thang

Bài 2.51. Giải phương trình nghiệm nguyên : $x^3 + 2y^3 = 4z^3$

Lời giải:

Từ phương trình ta thấy x là số chẵn, đặt $x = 2x_1$ được phương trình:

$$8x_1^3 + 2y^3 = 4z^3.$$

Chia hai vế cho 2, ta được $4x_1^3 + y^3 = 2z^3$. Suy ra được y chẵn, đặt $y = 2y_1$ được : $4x_1^3 + 8y_1^3 = 2z^3$.

Chia hai vế cho 2 được $2x_1^3 + 4y_1^3 = z^3$. Suy ra z chẵn. Đặt $z = 2z_1$ được

$$2x_1^3 + 4y_1^3 = 8z_1^3.$$

Chia hai vế cho 2 được $x_1^3 + 2y_1^3 = 4z_1^3$.

Tương tự ta có cả ba số x_1, y_1, z_1 đều chẵn. Từ đó ta đặt $x_1 = 2x_2$, $y_1 = 2y_2$, $z_1 = 2z_2$, với x_2, y_2, z_2 thỏa mãn phương trình $x_2^3 + 2y_2^3 = 4z_2^3$.

Giả sử x, y, z đồng thời chia hết cho 2^n, với n là một số nguyên dương nào đó. Khi đó $x = 2^2x_n$, $y = 2^2y_n$, $z = 2^nz_n$, với x_n, y_n, z_n thỏa mãn phương trình

$$x_n^3 + 2y_n^3 = 4z_n^3$$

Lập luận tương tự như trên ta có được x, y, z đồng thời chia hết 2^{n+1}. Theo quy nạp ta có x, y, z đồng thời chia hết cho 2^n với mọi n. Điều nảy chỉ xảy ra khi $x = 0$, $y = 0$, $z = 0$.

Vậy nghiệm của phương trình là (0, 0, 0).

Bài 2.52. Giải phương trình $8x^4 + 4y^4 + 2z^4 = t^4$

Lời giải :

Giả sử (x_0, y_0, z_0, t_0) là một nghiệm của phương trình, với điều kiện $x_0 > 0$ là nghiệm nhỏ nhất. Khi đó ta có phương trình $8x_0^4 + 4y_0^4 + 2z_0^4 = t_0^4$

Từ phương trình trên ta thấy t_0 chẵn, đặt $t_0 = 2t_1$. Thế vào phương trình ta được : $4x_0^4 + 2y_0^4 + z_0^4 = 8t_1^4$

Ta lại thấy z_0 chẵn, đặt $z_0 = 2z_1$. Thế vào phương trình ta được

$$2x_0^4 + y_0^4 + 8z_1^4 = 4t_1^4$$

Lại có y_0 chẵn, đặt $y_0 = 2y_1$. Thế vào phương trình trên ta được

$$x_0^4 + 8y_1^4 + 4z_1^4 = 2t_1^4$$

Khi đó x_0 cũng chẵn, đặt $x_0 = 2x_1$, ta được phương trình

$$8x_1^4 + 4y_1^4 + 2z_1^4 = t_1^4.$$

Do đó (x_1, y_1, z_1, t_1) cũng là nghiệm của phương trình ban đầu, mà $x_1 < x_0$ trái với giả thiết x_0 là nghiệm nhỏ nhất.

Vậy phương trình có nghiệm duy nhất (0, 0, 0, 0).

2.6. Phương trình và hệ phương trình đồng dư bậc nhất một ẩn.

*) *Phương trình đồng dư bậc nhất một ẩn*: có dạng $ax \equiv b \pmod m$ (1), với a, b là các số nguyên , $a \neq 0 \pmod m$. Phương trình (1) luôn đưa được về dạng $ax \equiv b \pmod m$ với (a, m) = 1, phương trình này có một nghiệm, ta tìm nghiệm đó bằng các phương pháp sau:

1. Thử qua một hệ thặng dư đầy đủ:

Vì (a, m) = 1 nên khi x chạy qua một hệ thặng dư đầy đủ modulo a thì ax + b cũng chạy qua một hệ thặng dư đầy đủ modulo a. Mỗi hệ thặng dư đầy đủ theo modulo a có k để $mk + b \equiv 0 \pmod a$. Vậy $ax \equiv b \pmod a \Leftrightarrow ax \equiv b + mk \pmod m$ $\Leftrightarrow x \equiv \frac{b+mk}{a} \pmod m$.

2. Áp dụng định lí Euler:

Theo định lí Euler thì $a^{\varphi(m)} \equiv 1 (\text{mod } m)$ nên $a.a^{\varphi(m)-1}b \equiv b (\text{mod } m)$. Do đó nghiệm của phương trình (1) là $x \equiv a^{\varphi(m)-1}b (\text{mod } m)$.

3. Áp dụng liên phân số:

Biểu diễn $\frac{m}{a} = [q_0; q_1, \ldots, q_n]$. Ta có $aP_{n-1} - mQ_{n-1} = (-1)^n$ nên $aP_{n-1} \equiv (-1)^n \pmod m$. Vậy nghiệm của phương trình là $x \equiv (-1)^n bP_{n-1} \pmod m$.

*) *Hệ phương trình đồng dư bậc nhất một ẩn:* có dạng

$$\begin{cases} x \equiv a_1 (\text{mod } m_1) \\ x \equiv a_2 (\text{mod } m_2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv a_k (\text{mod } m_k) \end{cases}$$

với $m_1, m_2, \ldots, m_k$ là những số nguyên lớn hơn 1 và $a_1, a_2, \ldots, a_k$ là những số nguyên tùy ý

Bài 2.53. Giải phương trình : $3x \equiv 2 \pmod 7$

Lời giải:

Thử trên hệ thặng dư đầy đủ modulo 7 là {-3, -2, -1, 0, 1 ,2 , 3}. Ta có k = 1 để mk + b = 7.1 + 2 = 9 ≡ 0 (mod 3). Vậy x ≡ 3 (mod 7).

Bài 2.54. Giải phương trình: 31x ≡ 22 (mod 128)

Lời giải:

Ta tìm số nguyên k sao cho 128k ≡ - 22 (mod 31). Khi đó x ≡ $\frac{22+128t}{31}$ (mod 128) là nghiệm của phương trình. Việc tìm k dẫn tới việc giải phương trình 4k ≡ 9 (mod 31).

Ta tìm t sao cho 31t ≡ - 9 (mod 4) ⇔ t ≡ 1 (mod 4).

Chọn t = 1, khi đó : k = $\frac{9+31t}{4} = 10$

Vậy nghiệm của phương trình là x = $\frac{22+128.10}{31} \equiv 42(\text{mod } 128)$

Bài 2.55. Giải phương trình sau bằng cách áp dụng định lí Euler : 13x ≡ 7 (mod 30)

Lời giải :

Ta có 30 = 2.3.5 nên $\varphi(30) = 30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 8.$

Áp dụng định lí Euler ta được nghiệm của phương trình là x ≡ 13^8.7 (mod 30).

Bài 2.56. Giải phương trình sau : 42x ≡ 17 (mod 157).

Lời giải :

Biểu diễn $\frac{157}{42}$ = [3; 1, 2, 1, 4, 2]. Khi đó $P_1 = 4$, $P_2 = 10$, $P_3 = 14$, $P_4 = 66$, $P_5 = 146$.

Vậy nghiệm của phương trình là x ≡ $(-1)^5$.17.66 (mod 157) ≡ 134 (mod 157).

Bài 2.57. Giải hệ phương trình đồng dư sau :

$$\begin{cases} x \equiv 26 \pmod{36} \\ x \equiv 2 \pmod{60} \\ x \equiv 92 \pmod{150} \end{cases}$$

Lời giải :

Xét hệ hai phương trình $\begin{cases} x \equiv 26 \pmod{36} \\ x \equiv 2 \pmod{60} \end{cases} \Leftrightarrow \begin{cases} x = 36t + 26 \\ 36t + 26 \equiv 2 \pmod{60} \end{cases}, t \in \mathbb{Z}$

Phương trình $36t + 26 \equiv 2 \pmod{60} \Leftrightarrow 36t \equiv 36 \pmod{60} \Leftrightarrow t \equiv 1 \pmod{5}$.

Vậy ta được nghiệm của hệ phương trình đang xét là :

$$x \equiv 36.1 + 26 \pmod{180} \equiv 62 \pmod{180}.$$

Do đó hệ phương trình đã cho tương đương với hệ phương trình :

$$\begin{cases} x \equiv 62 \pmod{180} \\ x \equiv 92 \pmod{150} \end{cases} \Leftrightarrow \begin{cases} x = 180t' + 62 \\ 180t' + 62 \equiv 92 \pmod{150} \end{cases}, t' \in \mathbb{Z}$$

Phương trình $180t' + 62 \equiv 92 \pmod{150} \Leftrightarrow 180t' \equiv 30 \pmod{150} \Leftrightarrow 6t' \equiv 1 \pmod{5} \Leftrightarrow t' \equiv 1 \pmod{5}$. Khi đó hệ phương trình đang xét có nghiệm là

$$x \equiv 180.1 + 62 \pmod{900} \equiv 242 \pmod{900}$$

Vậy hệ phương trình có nghiệm là $x \equiv 242 \pmod{900}$.

Bài 2.58. Một bài toán dân gian :

Nguyên Tiêu gió mát trăng trong

Phố phường nhộn nhịp đèn chong sáng lòa

Một mình dạo đếm đèn hoa

Dăm trăm đốm sáng biết là ai hay

Kết năm chẵn số đèn này

Bảy đèn kết một còn ba ngọn thừa

Chín đèn thì bốn ngọn dư

Đèn bao nhiêu ngọn mà ngơ ngẩn lòng ?

Lời giải :

Bài toán cho ta hệ phương trình

$$\begin{cases} x \equiv 0 \pmod 5 \\ x \equiv 2 \pmod 7 \\ x \equiv 4 \pmod 9 \end{cases}$$

Áp dụng định lí phần dư Trung Hoa, ta có m = 5.7.9 = 315.

$M_1 = 7.9 = 63$ nên ta có $63y_1 \equiv 1 \pmod 5$, suy ra $y_1 = 2$.

$M_2 = 5.9 = 45$ nên ta có $45y_2 \equiv 1 \pmod 7$, suy ra $y_2 = 5$.

$M_3 = 7.5 = 35$ nên ta có $35y_3 \equiv 1 \pmod 9$, suy ra $y_3 = 8$.

Ta được nghiệm của hệ phương trình đã cho là

$x \equiv 2.63.0 + 5.45.2 + 8.35.4 \pmod{315}$ hay $x \equiv -5 \pmod{315}$.

Vậy số đèn đếm được hoặc là 310 hoặc là 625.

Chương 3. Hàm số học

3.1. Kiến thức cơ bản

Hàm số học là hàm nhận được giá thị thực hoặc phức và xác định trên tập số nguyên dương.

Hàm số học f không đồng nhất bằng 0, được gọi là có tính nhân nếu $f(mn) = f(m)f(n)$, với $(m, n) = 1$. Hàm số học f không đồng nhất bằng 0, được gọi là có tính nhân đầy đủ nếu nếu $f(mn) = f(m)f(n)$, với mọi số nguyên dương m, n.

3.1.1. Hàm Euler $\varphi(n)$

Phi –hàm Euler, kí hiệu φ, được xác định bởi : $\varphi(n)$ là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n.

Định lý 3.1.1 Phi – hàm Euler có tính nhân.

Bổ đề 3.1.1 Giả sử m, n là các số nguyên dương nguyên tố cùng nhau; $\{a_i: 1 \le i \le m\}$ và ; $\{b_j: 1 \le j \le n\}$ tương ứng là các hệ thặng dư đầy đủ modulo m và n. Khi đó ta có ; $\{a_i n + b_j : 1 \le i \le m, 1 \le j \le n\}$ là thế hệ thặng dư đầy đủ modulo mn.

Chứng minh. Bây giờ chúng ta chứng minh định lý.

Vì $(m , n) = 1$ nên $\varphi(mn)$ là các số phần tử của hệ $\{a_i n + b_j m: 1 \le i \le m, 1 \le j \le n\}$, thỏa $(a_i n + b_j m, mn) = 1$.

Nhưng $(a_i n + b_j m, mn) = 1$ tương đương với

$$\begin{cases} (a_i n + b_j m, m) = 1 \\ (a_i n + b_j m, n) = 1 \end{cases} \Leftrightarrow \begin{cases} (a_i n , m) = 1 \\ (b_j m, n) = 1 \end{cases} \Leftrightarrow \begin{cases} (a_i , m) = 1 \\ (b_j, n) = 1 \end{cases}$$

Vì có $\varphi(m)$ các a_i thỏa $(a_i , m) = 1$ và $\varphi(n)$ các b_j thỏa $(b_j, n) = 1$ nên có cả thảy $\varphi(m)\ \varphi(n)$ các $a_i n + b_j m$ thỏa $(a_i n + b_j m, mn) = 1$.

Định lý 3.1.2.Nếu p nguyên tố và α nguyên dương thì $\varphi(p^\alpha) = p^\alpha\left(1-\frac{1}{p}\right)$.

Chứng minh. Các số nguyên dương không vượt quá p^α và không nguyên tố cùng nhau với p^α chính là các số nguyên dương không vượt quá p^α và chia hết cho p. Đó chính là các số kp mà $1 \le k \le p^{\alpha-1}$. Có cả thảy $p^{\alpha-1}$ số như vậy, do đó $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1-1/p)$.

Định lí 3.1.3. Nếu $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ là khai triển lũy thừa nguyên tố của số nguyên dương n thì

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_{2)}}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

Định lý 3.1.4. Nếu n là số nguyên dương thì: $\sum_{d/n}\varphi(d) = n$.

Chứng minh. Chúng ta phân các số nguyên m từ 1 đến n thành các lớp C_d. Số nguyên m, $1 \le m \le n$ thuộc lớp C_d nếu $(m,n) = d$ thế thì $m \in C_d$ khi và chỉ khi $(m/d, n/d) = 1$. Như vậy mỗi lớp C_d có đúng $\varphi(n/d)$ số. Vậy

$$n = \sum_{d/n}\varphi(n/d) = \sum_{d/n}\varphi(d).$$

3.1.2. Hàm tổng các ước $\sigma(n)$ và các số ước $\tau(n)$.

Hàm tổng các ước, ký hiệu bởi σ, được xác định bởi : $\sigma(n)$ là tổng tất cả các ước dương của số nguyên dương n.

Hàm số các ước, ký hiệu bởi τ, được xác định bởi: $\tau(n)$ là số các ước dương của số nguyên dương n.

Định lý 3.1.5. Các hàm σ và τ có tính nhân.

Định lý 3.1.6. Nếu $n = p_1^{\alpha_1}p_2^{\alpha_2}....p_k^{\alpha_k}$ là khai triển luỹ thừa nguyên tố của số nguyên dương n thì

$$\sigma(n)=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1} \quad (1); \qquad \tau(n)=\prod_{i=1}^{k}(\alpha_i+1) \quad (2)$$

Chứng minh.

(1) Vì p^α chỉ có $(\alpha+1)$ ước dương là $p^i, 0\le i\le\alpha$ nên

$$\sigma(p^\alpha)=1+p+\cdots+p^\alpha=\frac{p^{\alpha+1}-1}{p-1}.$$

Vậy $$\sigma(n)=\prod_{i=1}^{k}\sigma(p_i^{\alpha_i})=\prod_{i=1}^{k}\frac{p^{\alpha_i+1}}{p_i-1}$$

(2) Vì p^α chỉ có $(\alpha+1)$ ước dương là $p^i, 0\le i\le\alpha$ nên $\tau(p^\alpha)=(\alpha+1)$. Vậy

$$\tau(n)=\prod_{i=1}^{k}\tau(p_i^{\alpha_i})=\prod_{i=1}^{k}(\alpha_i+1)$$

3.2. Các bài toán về hàm số học

Bài 3.1. Tìm các số tự nhiên n biết dạng phân tích tiêu chuẩn $n = 2^a3^b$ và $\tau(n) = 14$.

Lời giải :

Áp dụng công thức tính $\tau(n)$ ta có

$\tau(n) = (a + 1)(b + 1)$

Theo đề bài thì $(a+1)(b+1) = 14 = 2.7 = 1.14$. Mà $\begin{cases} a+1\ge 2 \\ b+1\ge 2 \end{cases}$ nên

$$\begin{cases} a+1=2 \\ b+1=7 \end{cases} \text{hoặc} \begin{cases} a+1=7 \\ b+1=2 \end{cases}. \text{ Khi đó} \begin{cases} a=1 \\ b=6 \end{cases} \text{hoặc} \begin{cases} a=6 \\ b=1 \end{cases}.$$

Vậy $n = 2.3^6 = 1457$ hoặc $n = 2^6.3 = 192$.

Bài 3.2. Tìm số tự nhiên n có dạng phân tích tiêu chuẩn $n = p^aq^b$ và $\tau(n) = 6, \sigma(n) = 28$.

Lời giải:

Ta có $\tau(n) = (a + 1)(b + 1) = 6$. Mà $\begin{cases} a + 1 \geq 2 \\ b + 1 \geq 2 \end{cases}$ nên

$$\begin{cases} a + 1 = 2 \\ b + 1 = 3 \end{cases} \text{ hoặc } \begin{cases} a + 1 = 3 \\ b + 1 = 2 \end{cases}.$$

+ Nếu $\begin{cases} a + 1 = 3 \\ b + 1 = 2 \end{cases}$ thì $\begin{cases} a = 2 \\ b = 1 \end{cases}$. Khi đó $n = p^2q$. Áp dụng công thức tính ta được

$\sigma(n) = (p^2 + p + 1)(q + 1) = 28 = 4.7 = 14.2 = 1.28$

Mà $\begin{cases} p^2 + p + 1 \geq 7 \text{ (vì } p^2 + p + 1 \text{ lẻ và } p \geq 2) \\ q + 1 \geq 3 \end{cases}$

$\Leftrightarrow \begin{cases} p^2 + p + 1 = 7 \\ q + 1 = 4 \end{cases} \Leftrightarrow \begin{cases} p = 2 \\ q = 3 \end{cases}$

Do đó $n = 2^2.3 = 12$

+ Nếu $\begin{cases} a + 1 = 2 \\ b + 1 = 3 \end{cases}$, làm tương tự ta cũng được kết quả $n = 12$.

Vậy số cần tìm là 12.

Bài 3.3. Tìm các số tự nhiên biết :

a. Dạng phân tích tiêu chuẩn $n = 2^a3^b$ và $\sigma(n) = 403$

b. Dạng phân tích tiêu chuẩn $n = 3p^2$ và $\sigma(n) = 124$.

Lời giải :

a. Ta có $\sigma(n) = (2^{a+1} - 1).\frac{3^{b+1}-1}{2}$

$\Leftrightarrow (2^{a+1} - 1)(3^{b+1} - 1) = 2.403 = 26.31 = 13.62$.

Khi đó $\begin{cases}2^{a+1}-1=26\\3^{b+1}-1=31\end{cases}$ hoặc $\begin{cases}2^{a+1}-1=31\\3^{b+1}-1=26\end{cases}$ hoặc $\begin{cases}2^{a+1}-1=13\\3^{b+1}-1=62\end{cases}$ hoặc $\begin{cases}2^{a+1}-1=62\\3^{b+1}-1=13\end{cases}$. Ta thấy chỉ có hệ $\begin{cases}2^{a+1}-1=31\\3^{b+1}-1=26\end{cases}$ có nghiệm $\begin{cases}a=4\\b=2\end{cases}$, các hệ còn lại vô nghiệm.

Vậy $n = 2^4.3^2 = 144$.

b. Ta có $\sigma(n) = \frac{3^2-1}{2}.\frac{p^3-1}{p-1}$

$\Leftrightarrow 4(p^2 + p + 1) = 124$

$\Leftrightarrow p^2 + p + 1 = 31$

$\Leftrightarrow \left[\begin{array}{l}p=5\\p=-6\ (\text{loại})\end{array}\right.$

Vậy $n = 3.25 = 75$.

Bài 3.4. Cho $n = p^aq^b$ là dạng phân tích tiêu chuẩn của n và $\tau(n^2) = 15$. Hãy tính $\tau(n^3)$?

(Trích tài liệu [4])

Lời giải :

Ta có $n^2 = p^{2a}q^{2b}$ nên $\tau(n^2) = (2a + 1)(2b + 1) \Leftrightarrow (2a + 1)(2b + 1) = 15$

Vì vai trò của a, b như nhau, nên ta chỉ cần giải một hệ

$\begin{cases}2a+1=3\\2b+1=5\end{cases} \Leftrightarrow \begin{cases}a=1\\b=2\end{cases}$.

Do đó $n = pq^2$, $n^3 = p^3q^6$ nên $\tau(n^3) = (3 + 1)(6 + 1) = 28$.

Vậy $\tau(n^3) = 28$

Bài 3.5. Tìm số tự nhiên n, biết:

a. Dạng phân tích tiêu chuẩn $n = 3^a5^b7^c$ và $\varphi(n) = 3600$

b. Dạng phân tích tiêu chuẩn $n = 2^a3^bp$ và $\varphi(n) = 180$

Lời giải:

a. Ta có $\varphi(n) = n(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{7})$

$\Leftrightarrow 3^a5^b7^c.\frac{16}{35} = 3600$

$\Leftrightarrow 3^a5^b7^c = 7875 = 3^2.5^3.7$. Suy ra a = 2, b = 3, c = 1

Vậy n = 7875

b. Ta có $\varphi(n) = n(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{p})$

$\Leftrightarrow 2^a3^b.\frac{p-1}{3} = 180$

$\Leftrightarrow 2^a3^{b-1}(p - 1) = 180 = 2.3^2.10 = 2.3.30$ (vì p là số nguyên tố khác 2, 3 nên p – 1 là hợp số). Do đó a = 1, b = 3, p = 11 hoặc a = 1, b = 2, p = 31.

Vậy $n = 2.3^3.11 = 594$ hoặc $n = 2.3^2.31 = 558$.

Bài 3.6. Tìm số tự nhiên n sao cho n chia hết cho $\varphi(n)$, với $\varphi(n)$ là hàm Euler

Lời giải:

Ta thấy n = 1 thì $\varphi(n) = 0$

Với n > 1. Giả sử n có phân tích tiêu chuẩn $n = p_1^{\alpha_1} p_2^{\alpha_2} ....p_k^{\alpha_k}$ thì

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right).$$

Vì n chia hết cho $\varphi(n)$ nên đặt $n = t.\varphi(n)$, với t là số tự nhiên bất kì. Khi đó ta được:

$p_1p_2...p_k = t(p_1 - 1)(p_2 - 1)... (p_k - 1)$

Ta thấy vế phải của đẳng thức trên chẵn nên phải có một p_i nào đó bằng 2 ($i = 1, 2, \ldots, k$). Giả sử là p_1, ta có:

$$2p_2 \ldots p_k = t(p_1 - 1)(p_2 - 1) \ldots (p_k - 1)$$

Do $p_2, p_3, \ldots, p_k$ khác 2 nên từ đẳng thức trên ta suy ra n có nhiều nhất một ước nguyên tố lẻ. Giả sử là p_2, đặt $p_2 = 2u + 1$, ta có $2p_2 = t(2u)$. Vì p_2 nguyên tố khác 2, suy ra $t = p_2$ và $u = 1$, suy ra $p_2 = 3$. Khi đó $n = 2^a 3^b$ với $a \geq 1, b \geq 0$.

Vậy $n = 1$ hoặc $n = 2^a 3^b$ với $a \geq 1, b \geq 0$ thì n chia hết cho $\varphi(n)$.

Bài 3.7. Chứng minh rằng

a. Nếu m chia hết cho n thì $\varphi(m)$ chia hết cho $\varphi(n)$.

b. $\varphi(m^a) = m^{a-1} \varphi(m)$.

Lời giải:

a. Giả sử n có dạng phân tích tiêu chuẩn là $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}$ vì m chia hết cho n nên m có dạng phân tích tiêu chuẩn là $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i} \ldots p_k^{\alpha_k}$, với $i \leq k$.

Khi đó: $\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_i}\right) \ldots (1 - \frac{1}{p_k})$

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_i}\right)$$

Vì m chia hết cho n, đặt $m = t.n$ thì

$$\varphi(m) = tn\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_i}\right) \ldots (1 - \frac{1}{p_k})$$

$$= \left[n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_i}\right)\right] t \ldots \left(1 - \frac{1}{p_k}\right)$$

$$= \varphi(n).\, t \ldots \left(1 - \frac{1}{p_k}\right)$$

Vậy $\varphi(m)$ chia hết cho $\varphi(n)$.

b. Giả sử m có dạng phân tích tiêu chuẩn là $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, thì

$m^a = p_1^{a\alpha_1} p_2^{a\alpha_2} \dots p_k^{a\alpha_k}$. Khi đó

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right).$$

$$\varphi(m^a) = m^a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right)$$

$$= m^{a-1}.m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right)$$

$$= m^{a-1}\varphi(m)$$

Vậy $\varphi(m^a) = m^{a-1}\varphi(m)$.

Bài 3.8. Chứng minh rằng với mọi số tự nhiên $n \geq 2$, ta luôn có

$$\sigma(n) + \varphi(n) \geq 2n$$

Lời giải :

Giả sử các ước của n là $d_1, d_2, \dots, d_k$ và $1 = d_1 < d_2 < \dots < d_k = n$

Ta thấy trong các số tự nhiên không vượt quá n có $\frac{n}{d_i}$ số là bội của d_i

(i = 1, 2, …, k).

Mà mỗi số không vượt quá n và không nguyên tố cùng nhau với n đều là bội của một ước nào đó lớn hơn 1 của n. Do đó ta có :

$$n - \varphi(n) \leq \frac{n}{d_2} + \frac{n}{d_3} + \dots + \frac{n}{d_k}$$

Lại có : $\frac{n}{d_2} + \frac{n}{d_3} + \dots + \frac{n}{d_k} = d_{k-1} + d_{k-2} + \dots + d_1 = \sigma(n) - d_k = \sigma(n) - n$

nên $n - \varphi(n) \leq \sigma(n) - n$, hay $\sigma(n) + \varphi(n) \geq 2n$

Dấu đẳng thức xảy ra khi n là số nguyên tố.

Vậy $\sigma(n) + \varphi(n) \geq 2n$, với mọi số tự nhiên $n \geq 2$.

Bài 3.9. Gọi m = [a, b], d = (a, b). Chứng minh rằng:

a. $\varphi(ab) = d\varphi(m)$

b. $\varphi(ab)\varphi(d) = d\varphi(a)\varphi(b)$

c. $\varphi(a)\varphi(b) = \varphi(m)\varphi(d)$

(Trích tài liệu [4])

Lời giải:

Giả sử $p_1, p_2, \ldots, p_i$ là các số nguyên tố chỉ có trong sự phân tích tiêu chuẩn của a; $q_1, q_2, \ldots, q_j$ là các số nguyên tố chỉ có trong sự phân tích tiêu chuẩn của b; $r_1, r_2, \ldots, r_k$ là các số nguyên tố có mặt trong cả hai sự phân tích tiêu chuẩn của a và b. Ta có:

$$\varphi(a) = a\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_i}\right)\left(1-\frac{1}{r_1}\right)\ldots\left(1-\frac{1}{r_k}\right)$$

$$\varphi(b) = b\left(1-\frac{1}{q_1}\right)\ldots\left(1-\frac{1}{q_j}\right)\left(1-\frac{1}{r_1}\right)\ldots\left(1-\frac{1}{r_k}\right)$$

$$\varphi(d) = d\left(1-\frac{1}{r_1}\right)\ldots\left(1-\frac{1}{r_i}\right)$$

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_i}\right)\left(1-\frac{1}{q_1}\right)\ldots\left(1-\frac{1}{q_j}\right)\left(1-\frac{1}{r_1}\right)\ldots\left(1-\frac{1}{r_k}\right)$$

$$\varphi(ab) = ab\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_i}\right)\left(1-\frac{1}{q_1}\right)\ldots\left(1-\frac{1}{q_j}\right)\left(1-\frac{1}{r_1}\right)\ldots\left(1-\frac{1}{r_k}\right)$$

a. Ta thấy $\varphi(ab) = ab\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_i}\right)\left(1-\frac{1}{q_1}\right)\ldots\left(1-\frac{1}{q_j}\right)\left(1-\frac{1}{r_1}\right)\ldots\left(1-\frac{1}{r_k}\right)$

$= p_1p_2\ldots p_iq_1q_2\ldots q_j\,(r_1r_2\ldots r_k)^2(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_i})(1-\frac{1}{q_1})\ldots(1-\frac{1}{q_j})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})$

$= (r_1r_2\ldots r_k)\,[p_1p_2\ldots p_iq_1q_2\ldots q_jr_1r_2\ldots r_k(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_i})(1-\frac{1}{q_1})\ldots(1-\frac{1}{q_j})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})\,]$

$= d\varphi(m)$

Vậy $\varphi(ab) = d\varphi(m)$

b. $\varphi(ab)\varphi(d) = abd\,(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_i})(1-\frac{1}{q_1})\ldots(1-\frac{1}{q_j})[(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})]^2$

$= p_1p_2\ldots p_iq_1q_2\ldots q_j\,(r_1r_2\ldots r_k)^3\,(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_i})(1-\frac{1}{q_1})\ldots(1-\frac{1}{q_j})[(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})]^2$

$= [r_1r_2\ldots r_k][p_1p_2\ldots p_ir_1r_2\ldots r_k\,(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_i})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})\,][\,q_1q_2\ldots q_jr_1r_2\ldots r_k$

$(1-\frac{1}{q_1})\ldots(1-\frac{1}{q_j})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})\,]$

$= d\varphi(a)\varphi(b)$

Vậy $\varphi(ab)\varphi(d) = d\varphi(a)\varphi(b)$

c. $\varphi(a)\varphi(b) = a(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_i})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})\,b$

$(1-\frac{1}{q_1})\ldots(1-\frac{1}{q_j})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})$

$= p_1p_2\ldots p_ir_1r_2\ldots r_k\,(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_i})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})\,q_1q_2\ldots q_jr_1r_2\ldots r_k$

$(1-\frac{1}{q_1})\ldots(1-\frac{1}{q_j})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})$

$= [p_1p_2\ldots p_iq_1q_2\ldots q_j\ r_1r_2\ldots r_k\ (1-\frac{1}{p_1})\ldots(1-\frac{1}{p_i})(1-\frac{1}{q_1})\ldots(1-\frac{1}{q_j})(1-\frac{1}{r_1})\ldots(1-\frac{1}{r_k})\ ][\ r_1r_2\ldots r_k\ (1-\frac{1}{r_1})\ldots(1-\frac{1}{r_i})\ ]$

$= \varphi(m)\varphi(d)$

Vậy $\varphi(a)\varphi(b) = \varphi(m)\varphi(d)$.

Bài 3.10. Chứng minh rằng $\sigma(n) = n + 1$ khi và chỉ khi n là số nguyên tố.

Lời giải:

Nếu n là số nguyên tố thì nó có hai ước là n và 1. Do đó $\sigma(n) = n + 1$

Mặt khác, nếu n là hợp số, đặt n = ab với a, b là các số tự nhiên lớn hơn 1. Khi đó n có ít nhất ba ước phân biệt là 1, a, n nên $\sigma(n) \geq 1 + a + n > n + 1$

Nếu n = 1 thì $\sigma(n) = 1 < 1 + 1$.

Vậy $\sigma(n) = n + 1$ khi và chỉ khi n là số nguyên tố.

KẾT LUẬN

Luận văn đã đạt được một số kết quả quan trọng sau:

- Luận văn đã hệ thống và phân loại một số dạng toán số học thường gặp. Thông qua hệ thống các bài tập cùng các lời giải với mỗi dạng

toán, luận văn đã cung cấp được một số phương pháp giải các dạng toán trong tập số nguyên, các dạng bài áp dụng lí thuyết đồng dư và hàm số học.

- Luận văn đã sưu tập được nhiều bài toán hay của các kì thi học sinh giỏi quốc gia, các tỉnh thành, Olympic toán các nước, …

Dù đã cố gắng hết sức trong quá trình làm luận văn, nhưng luận văn khó tránh khỏi những thiếu xót nhất định. Em rất mong nhận được sự chỉ bảo của quý thầy cô và những góp ý của bạn đọc để luận văn được hoàn thiện.

Tài liệu tham khảo

[1] Các đề thi Olympic toán các nước

[2] Các đề thi tuyển sinh THPT chuyên, 2000 – 2014

[3] Đặng Huy Ruận, *Phương pháp giải bài toán chia hết*, Nhà xuất bản khoa học và kĩ thuật

[4] Nguyễn Hữu Hoan, *Lí thuyết số*, Nhà xuất bản Đại học sư phạm

[5] Nguyễn Vũ Thành, *Chuyên đề bồi dưỡng học sinh giỏi toán THCS Số học*, Nhà xuất bản giáo dục

[6] Website: diendantoanhoc.net