CHỦ ĐỀ: SỐ HỌC

Thời gian làm bài: 180 phút

Bảng PT

A. Khái niệm cấp

Bài PT.1. Xét luỹ thừa a^m ($m \geq 1$). Do chỉ có một số hữu hạn các lớp đồng dư modulo n (có n lớp cả thảy) nên phải tồn tại $m_1 > m_2$ để $a^{m_1} \equiv a^{m_2} \pmod{n}$. Do $(a, m) = 1$ đồng dư này dẫn đến $a^{m_1 - m_2} \equiv 1 \pmod{n}$. Như vậy, tập các số nguyên dương k sao cho $a^k \equiv 1 \pmod{n}$ là không rỗng, nói riêng có một phần tử nhỏ nhất c.

Bài PT.2. Nếu $c = \mathrm{ord}_n(a) \mid k$ thì rõ ràng $p \mid a^c - 1 \mid a^k - 1$. Đảo lại, giả sử k là một số nguyên dương thoả mãn $a^k \equiv 1 \pmod{n}$. Viết $k = cq + r$ với $0 \leq r < c$. Thế thì $1 \equiv a^k = (a^c)^q \cdot a^r \equiv a^r \pmod{p}$. Từ định nghĩa của c ta phải có $r = 0$, nghĩa là $c \mid k$.

Bài PT.3. Theo định lý Euler, $a^{\phi(n)} \equiv 1 \pmod{n}$. Từ đó, kết luận của bài toán PT.2 cho thấy $c \mid \phi(n)$.

B. Sự tồn tại số nguyên tố trong một số cấp số cộng

Bài PT.4. Giả sử chỉ tồn tại hữu hạn số nguyên tố $p_1, \ldots, p_n$ có dạng $4k+1$. Xét số $4\prod_{i=1}^{n} p_i - 1$. Số này nhất thiết phải có một ước nguyên tố dạng $4k + 3$. Nhưng ước nguyên tố này không thể là một trong các p_i, vô lý.

Bài PT.5. (i) Giả sử $p \mid n^2 + 1$, p nguyên tố $\equiv 3 \pmod{4}$. Theo định lý Fermat nhỏ $n^{p-1} \equiv 1 \pmod{p}$, nghĩa là $(-1)^{2k+1} \equiv 1 \pmod{p}$, vô lý.

(ii) Giả sử chỉ có một số hữu hạn các số nguyên tố $\equiv 1 \pmod{4}$, là $p_1, \ldots, p_n$. Xét số $\left(2\prod_{i=1}^{n} p_i\right)^2 + 1$. Theo (i), một ước nguyên tố bất kì của số này (hiển nhiên là lẻ) đều $\equiv 1 \pmod{4}$ và không thể là một trong các p_i được, vô lý.

Bài PT.6. (i) Xét $p \mid n^2 - n + 1$, nguyên tố, $p \neq 3$. Chú ý rằng do $n^2 + n - 1$ là lẻ, ta phải có $n \equiv 1 \pmod{6}$ hoặc $n \equiv 5 \pmod{6}$. Giả sử $p \equiv 5 \pmod{6}$. Ta có $n^3 \equiv -1 \pmod{p}$. Từ đó

$$n^{p-1} \equiv n^{6k+4} \equiv (-1)n \pmod{p}.$$

Kết hợp với định lý Fermat nhỏ, ta suy ra $n \equiv -1 \pmod{p}$. Thế nhưng khi đó $n^2 - n + 1 \equiv 3 \pmod{p}$, vô lý.

(ii) Giả sử chỉ có hữu hạn số nguyên tố $\equiv 1 \pmod 6$ là $p_1, \ldots, p_r$. Xét $n = 3\prod_{i=1}^{r} p_i$. Khi đó một ước nguyên tố của $n^2 - n + 1$ (hiển nhiên $\neq 3$) đều $\equiv 1 \pmod 6$ và khác các ước p_i, vô lý.

C. Sự tồn tại số nguyên tố trong cấp số cộng dạng $nk + 1$

Bài PT.7. Chú ý rằng $p \mid k^k - 1$ nên $(k, p) = 1$ và theo tính chất về cấp thì $c \mid k$. Đặt $k = ck'$. Như vậy,

$$k^k - 1 = k^{ck'} - 1 = (k^c - 1)(k^{c(k'-1)} + k^{c(k'-2)} + \cdots + 1).$$

Bởi vì $k^c \equiv 1 \pmod p$, và chú ý rằng $(p, k') = 1$, nên ta có

$$k^{c(k'-1)} + k^{c(k'-2)} + \cdots + 1 \equiv 1 + 1 + \cdots + 1 = k' \not\equiv 0 \pmod p.$$

Như vậy, $k^k - 1$ là tích của $k^c - 1$ với một số nguyên không chia hết cho p. Vì vậy, $v_p(k^k - 1) = v_p(k^c - 1)$.

Lưu ý rằng, với mọi d sao cho $c \mid d \mid k$ thì $k^c - 1 \mid k^d - 1 \mid k^k - 1$ nên rõ ràng ta cũng phải có $v_p(k^c - 1) = v_p(k^d - 1) = v_p(k^k - 1)$.

Bài PT.8. Ta vẫn ký hiệu c cho cấp của k modulo p. Ta biết rằng với mọi d, $p \mid k^d - 1$ khi và chỉ khi $c \mid d$. Hơn nữa, nếu ta đặt $v = v_p(k^k - 1)$ thì theo nhận xét cuối của trong lập luận của bài toán PT.7 ở trên, với mọi $d \in \mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$,

$$p \mid k^d - 1 \implies v_p(k^d - 1) = v.$$

Từ đó suy ra, $v_p(A) = s_a v, v_p(B) = s_b v$, trong đó s_a (tương ứng, s_b) kí hiệu số các phần tử $d \in \mathcal{D}_1$ (tương ứng, $d \in \mathcal{D}_2$) sao cho $c \mid d$, nói cách khác, sao cho $\frac{k}{d}$ là ước của $\frac{k}{c}$.

Chú ý rằng theo định lý Fermat nhỏ $c \mid p - 1$ nên nếu $c = k$ thì $k \mid p - 1$ hay $p \equiv 1 \pmod k$, trái với giả thiết bài toán. Như vậy, $c < k$. Ta kí hiệu $q_1, \ldots, q_N$ là tất cả các ước nguyên tố phân biệt của $\frac{k}{c}$ (như vậy, $N \geq 1$). Thế thì s_a bằng số các cách chọn $1, 3, \ldots,$ phần tử của tập $\{q_1, \ldots, q_N\}$, nói cách khác, bằng $\binom{N}{1} + \binom{N}{3} + \cdots = \frac{1}{2}\left[(1+1)^N - (1-1)^N\right] = 2^{N-1}$. Tương tự, s_b bằng số các cách chọn $2, 4, \ldots,$ phần tử của tập $\{q_1, \ldots, q_N\}$ (chú ý điều kiện $d \neq k$, hay $\frac{k}{d} \neq 1$), do đó bằng $\frac{1}{2}\left[(1+1)^N + (1-1)^N\right] - 1 = 2^{N-1} - 1$. Ta suy ra $v_p(A) = 2^{N-1}v = v_p(B) + v_p(k^k - 1)$.

Bài PT.9. Ta suy luận bằng phản chứng. Giả sử mọi ước nguyên tố của $k^k - 1$ đều $\not\equiv 1 \pmod k$. Chú ý rằng mọi ước nguyên tố của A và B đều là ước nguyên tố của một nhân tử có dạng $k^d - 1$ với $d \mid k$ nào đó nên cũng là ước của $k^k - 1$. Vì thế, theo kết luận của bài toán PT.8 ở trên, ta phải có

$$A = (k^k - 1)B. \quad (*)$$

Bây giờ, chú ý rằng $\mathcal{D} \neq \emptyset$ nên ta có thể chọn d_0 là phần tử nhỏ nhất của $\mathcal{D} = \mathcal{D}_1 \sqcup \mathcal{D}_2$. Thế thì mọi $d \in \mathcal{D}, d \neq d_0$ ta có $d > d_0$ và $k^d - 1 \equiv -1 \pmod{k^{d_0+1}}$, cũng như $k^k - 1 \equiv -1 \pmod{k^{d_0+1}}$. Như vậy, trong đẳng thức $(*)$ ở trên, mỗi nhân tử, ngoại trừ nhân tử $k^{d_0} - 1$, đều $\equiv -1 \pmod{k^{d_0+1}}$. Chính vì vậy, rút gọn $(*)$ modulo k^{d_0+1} cho ta $(-1)^r \equiv (-1)^s(k^{d_0} + 1) \pmod{k^{d_0+1}}$ với r, s nào đó. Thế nhưng hiển nhiên đồng dư trên không thể xảy ra. Điều mâu thuẫn này chứng tỏ sự tồn tại của một ước nguyên tố của $k^k - 1$ đồng dư với 1 modulo k.

Bài PT.10. Việc tồn tại vô hạn số nguyên tố lẻ là hiển nhiên (chẳng hạn được suy ra từ PT. 4) nên ta sẽ giả sử $k \geq 3$. Kết luận của bài toán PT.9 cho thấy tồn tại ít nhất một số nguyên tố $\equiv 1 \pmod{k}$. Giả sử chỉ tồn tại một số hữu hạn các số nguyên tố có dạng như vậy và gọi $p = kn_0 + 1$ là số nguyên tố lớn nhất trong các số nguyên tố $\equiv 1 \pmod{k}$. Thế nhưng, vẫn theo kết luận của PT.9, bây giờ áp dụng cho kn_0 thay vì k, có ít nhất một số nguyên tố $q \equiv 1 \pmod{2kn_0}$. Thế nhưng khi đó $q \equiv 1 \pmod{k}$ và $q > p$, mâu thuẫn với tính cực đại của p.