

VNU-HUS MAT3500: Toán rời rạc

Bài tập Lý thuyết số cơ bản II

Hoàng Anh Đức

Bộ môn Tin học, Đại học KHTN, ĐHQG Hà Nội
hoanganhduc@hus.edu.vn

Bài tập 1. Giải phương trình $15x^2 + 19x \equiv 5 \pmod{11}$. (**Gợi ý:** Chứng minh rằng phương trình đã cho tương đương với $15x^2 + 19x + 6 \equiv 0 \pmod{11}$). Phân tích vế trái của phương trình này thành nhân tử. Phương trình có nghiệm khi nào? Tại sao? Xem lại Bài tập 4 trong slides “Lý thuyết số cơ bản I”.)

Bài tập 2. Giải hệ phương trình sau bằng hai phương pháp đã đề cập trong bài giảng (sử dụng chứng minh của Định lý Phần dư Trung Hoa hoặc phương pháp thay thế ngược)

$$x \equiv 1 \pmod{2} \tag{1}$$

$$x \equiv 2 \pmod{3} \tag{2}$$

$$x \equiv 3 \pmod{5} \tag{3}$$

$$x \equiv 4 \pmod{11} \tag{4}$$

Bài tập 3 (*). Giải hệ phương trình

$$x \equiv 5 \pmod{6} \tag{5}$$

$$x \equiv 3 \pmod{10} \tag{6}$$

$$x \equiv 8 \pmod{15} \tag{7}$$

Chú ý: 6, 10, và 15 *không* đôi một nguyên tố cùng nhau.

Bài tập 4. Những số nguyên nào chia 2 dư 1 và chia 3 cũng dư 1?

Bài tập 5. Sử dụng Định lý Fermat nhỏ để tính

(a) $7^{121} \pmod{13}$

(b) $23^{1002} \pmod{41}$

(c) nghịch đảo của 5^{39} theo môđun 41

Bài tập 6. Sử dụng sự trợ giúp từ Định lý Fermat nhỏ, hãy chứng minh rằng 42 là ước của $n^7 - n$.