

# IT-math F2003 : Classroom Exercises

## Episode 5, March 4, 2003

1. Show that  $a \equiv b \pmod{n}$  iff  $b \equiv a \pmod{n}$ .
2. Let  $n \in \mathbb{Z}_+$ . Show that the integers  $r_1, r_2, s_1$  and  $s_2$  are such that  $r_1 \equiv r_2 \pmod{n}$  and  $s_1 \equiv s_2 \pmod{n}$ , then  $r_1 + s_1 \equiv r_2 + s_2 \pmod{n}$ .
3. Does  $[r]_n^{[s]_n} = [r^s]_n$  define an operation on the congruence classes modulo  $n$ ?
4. (a) Determine whether 13 is the inverse of 54 modulo 71 (i.e. determine whether  $[13]_{71}$  is the inverse of  $[54]_{71}$  in  $\mathbb{Z}_{71}$ );  
(b) Find the inverse of 54 modulo 71.

# IT-math F2003 : Homework Exercises

## Episode 5, March 4, 2003

### Fisherperson's Exercises

- Find out if 14 is the inverse of 17 modulo 31;
  - Find the inverse of 14 modulo 31;
  - Solve  $14 \cdot x \equiv 17 \pmod{31}$ .
- [the textbook, Exercise 2.3.20]** Write down the full list of units of  $\mathbb{Z}_{16}$ , and with each unit give its (multiplicative) inverse.
- Show that  $[n - 1]_n$  is a unit of  $\mathbb{Z}_n$  for any integer  $n \geq 2$ .

### Snake-Charmer's Exercises

- Find an integer solution of  $36x + 30y = -12$ .
- Show that if  $a \neq 0$  and  $\gcd(a, b) = \gcd(a, c) = 1$  then  $\gcd(a, b \cdot c) = 1$ .
- Suppose that  $[r]_n \in \mathbb{Z}_n$  is a unit (i.e. has an inverse) and that  $[m]_n \in \mathbb{Z}_n$ . Show that, if  $[r]_n \cdot [m_1]_n = [r]_n \cdot [m_2]_n$ , then  $[m_1]_n = [m_2]_n$ .

### Lion-Hunter's Exercises

- Show that if  $\gcd(a, c) = 1$  and  $c \mid a \cdot b$ , then  $c \mid b$ .
- Show that for non-zero integers  $a$  and  $b$ , the numbers  $\frac{a}{\gcd(a, b)}$  and  $\frac{b}{\gcd(a, b)}$  are relatively prime:  $\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1$ .
- Show that inverses in  $\mathbb{Z}_n$  are unique: if  $[r]_n \cdot [s_1]_n = [r]_n \cdot [s_2]_n = [1]_n$ , then  $[s_1]_n = [s_2]_n$ .

### Dragonslayer's Exercise

- Show that  $42 \mid b^7 - b$  for any integer  $b$ .