

Assignment 5/MATH 338/Fall, 2009  
Due: Monday, October 26

**General remarks:** 1. For the calculations, use a calculator. However, only integers should ever be

calculated. For instance, one often needs the integer  $\lfloor \frac{m}{n} \rfloor$ , the *floor* (integer part) of the fraction  $\frac{m}{n}$ ,

but never the decimal expansion of  $\frac{m}{n}$ .

**[1]** Give the complete prime factorization of all the integers  $a$  in the range  $720 \leq a \leq 730$ . Give sufficient reasons for your answers.

**[2]** Let  $a$ ,  $b$  and  $c$  be integers (in  $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$ ). We define, for positive or negative integers  $a$  and  $b$ , the gcd of them as

$\gcd(a, b) = \gcd(|a|, |b|)$ , and also  $\gcd(a, 0) = |a|$ ,  $\gcd(b, 0) = |b|$ , including  $\gcd(0, 0) = 0$ .

Consider the linear Diophantine equation

$$ax + by = c \quad (*)$$

( $x$  and  $y$  are integer unknowns; they have to be found in  $\mathbb{Z}$ ).

**Prove** that the Diophantine equation (\*) is solvable if and only if  $\gcd(a, b) \mid c$ .

(Recall that  $ax + by = d$  is solvable in integers when  $a$  and  $b$  are positive, and  $d = \gcd(a, b)$ .)

**[3]** 1) Use the Euclidean algorithm to **calculate**  $\gcd(a, b)$  for  $a = 161,995$  and  $b = 666,775$ .

2) Use the result, and also the intermediate results, of the calculation to

**2.1)** give a complete prime factorization of both  $a$  and  $b$ ;

**2.2)** give a particular solution of each of the linear Diophantine equations

$$ax + by = \cancel{1969}, \quad ax + by = \cancel{1968}$$

$1790$  $1791$

whichever is solvable ( $a$  and  $b$  are as in 1);  $x$  and  $y$  are integer unknowns in

and

**2.3) reduce** the fraction  $\frac{161,995}{666,775}$  to lowest terms.

(**Advice:** use the symbols  $a_0$  for  $a$ ,  $a_1$  for  $b$ , and  $a_2, a_3, \dots$  for the later remainders in the Euclidean algorithm, to make the writing shorter.)

**[4]** In this question,  $a, b, c, d, e, f, g, h, k, l$  always denote positive integers.

**1) Prove** that  $\gcd(a, b, c) = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) = \gcd(b, \gcd(a, c))$ .

**Instructions:**

To have a more convenient notation, write  $a \wedge b$  for  $\gcd(a, b)$ , and similarly for the other  $\gcd$ 's.

Use the following characterization, *learned in class*, of  $e \wedge f = \gcd(e, f)$ :  $g = e \wedge f$  is the unique positive integer for which

$$g | e \text{ and } g | f;$$

and

$$\text{for all } h, \text{ if } h | e \text{ and } h | f, \text{ then } h | g,$$

and **prove** that  $k = \gcd(\gcd(a, b), c) = (a \wedge b) \wedge c$  (the second form is the shorter notation) satisfies the following:

$$k | a, k | b \text{ and } k | c;$$

and

$$\text{for all } l, \text{ if } l | a, l | b \text{ and } l | c, \text{ then } l | k.$$

**Note** why the last fact implies that  $k$  is the *greatest* common divisor of the three numbers  $a, b$  and  $c$ .

Finally, **note** why the third and fourth terms in the equality above are also equal to  $\gcd(a, b, c)$  -- but without repeating steps of proofs done earlier.

**2) Prove** that there are (possibly zero or negative) integers  $x, y, z$  such that  $\gcd(a, b, c) = ax + by + cz$ .

**Hints:** recall and use the analogous fact for the gcd of two numbers, and use part 1).

**3) Calculate**  $\gcd(a,b,c)$  for  $a=962,053$ ,  $b=1,780,516$ ,  $c=1,437,284$ , and find  $x,y,z$  in  $\mathbb{Z}$  such that  $\gcd(a,b,c) = ax + by + cz$ .

(The numbers are large; however, the calculations will not be unreasonably long. This is a good example for seeing the efficiency of the Euclidean algorithm.)

**[5]** Let  $a$ ,  $b$  and  $c$  be integers (in  $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$ ), and let  $d = \gcd(a,b) = \gcd(|a|, |b|)$ . Consider the linear Diophantine equation

$$ax + by = c \quad (*)$$

( $x$  and  $y$  are integer unknowns; in  $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$ ).

**1)** Suppose that  $d$  is non-zero (equivalently, at least one of  $a$  and  $b$  is non-zero), and suppose that  $(x_0, y_0)$  is a particular solution of the Diophantine equation (\*). Let  $A = \frac{a}{d}$  and  $B = \frac{b}{d}$ . **Prove** that the general solution of (\*) is

$$x = x_0 + Bt, \quad y = y_0 - At$$

with a free *integer* variable (parameter)  $t$ . (This means that for any  $t$ , the formulas give a solution  $(x, y)$ ; and any solution  $(x, y)$  is so given by some  $t$ .)

**2)** Give the general solution of each of the Diophantine equations  $76x - 92y = 8$ ,  $76x - 92y = 7$ , whichever is solvable.

**3)** Give the general solution of each of the Diophantine equations

$$ax + by = 1969, \quad ax + by = 1968$$

~~1969~~  
1790 ~~1968~~  
1791

whichever is solvable; here  $a$  and  $b$  are as in question [3]. (see [3] 2.2))

**[6]** Consider the linear Diophantine equation

$$ax + by + cz = d \quad (**)$$

in the three integer unknowns  $x, y$  and  $z$ . Let  $D = \gcd(a, b, c)$ .

- 1) **Prove** that  $(**)$  is solvable in integer unknowns  $x, y$  and  $z$  if and only if  $D | d$ .
- 2) **Find** a particular solution of  $(**)$  when  $a, b$  and  $c$  are as in [4] 3), and  $d = 1038$ .
- 3)\* (for bonus points) Find the general solution of  $(**)$  for  $a, b, c$  and  $d$  as in 2).

[7] 1) **Prove** that  $\text{lcm}(a, b, c) = \text{lcm}(\text{lcm}(a, b), c)$ .

**Hint:** imitate, with the obvious changes, the proof given for [4] 1). Write  $a \vee b = \text{lcm}(a, b)$ .

2) **Calculate**  $\text{lcm}(a, b, c)$  for  $a, b$  and  $c$  given in [4] 3).

(Recall that the *least common multiple*,  $\text{lcm}(a, b)$ , of two positive integers  $a$  and  $b$  is the least

positive integer  $c$  such that  $a | c$  and  $b | c$ . We learned in class that  $\text{lcm}(a, b) = \frac{ab}{d} = \frac{a}{d} \cdot b = a \cdot \frac{b}{d}$

with  $d = \gcd(a, b)$ , and that  $\text{lcm}(a, b)$  divides every common multiple of  $a$  and  $b$ . (This is the content of Euclid's Propositions VII.34 and VII.35).)

3) With  $a, b$  and  $c$  as in 2), and  $u, v, w$  variable integers, **give** a formula for  $\frac{u}{a} + \frac{v}{b} + \frac{w}{c}$  in the form  $\frac{P}{q}$ , where  $q$  is a numerical integer, chosen as small as possible, and  $P$  is an expression of the form  $Au + Bv + Cw$ , with  $A, B, C$  (numerical) integers.

[8] We say that integers  $a$  and  $b$  are *relatively prime*, or *coprime*, if  $\gcd(a, b) = 1$ .

Similarly,  $a, b$  and  $c$  are *relatively prime (coprime)* if  $\gcd(a, b, c) = 1$ . *Equivalently*: two or three or more numbers are relatively prime if they do not have any common prime divisor.

**Prove** the following facts:

1)  $a$  and  $b$  are relatively prime if and only if  $a^2$  and  $b^2$  are relatively prime.

2) If  $p$  and  $q$  are coprime, and one of them is even, then the three

numbers  $p^2 + q^2$ ,  $p^2 - q^2$ ,  $2pq$  are relatively prime (note that the three numbers mentioned form a Pythagorean triple; if  $p$  and  $q$  are coprime, they form a primitive Pythagorean triple).

3) For any three positive integers  $a, b$  and  $c$ , we can find a unique triple of positive integers  $d, e$  and  $f$  such that  $a:b:c = d:e:f$  and  $d, e$  and  $f$  are relatively prime.